



info fedramp <info@gsa.gov>

[RAR] Submission of RAR for Client IronNet

1 message

(b) (6) (b) (6)@kratosdefense.com>
To: "Info@fedramp.gov" <Info@fedramp.gov>

Fri, May 15, 2020 at 4:50 PM

FedRAMP PMO,

Kratos is the 3PAO for the IronNet (CSP) client seeking consideration for a FedRAMP Ready (RAR) status.

Pursuant to the readiness status Kratos is requesting a doc folder/repository on OMB MAX for IronNet (CSP).

Please notify Kratos when said repository ready for use.

Sincerely, (b) (6)

Kratos | Chandler, AZ | TTS-Cyber Principal Security Consultant

C: (b) (6) | www.kratossecureinfo.com





info fedramp <info@gsa.gov>

IronNet RAR Evaluation Form - Signed

1 message

(b) (6) <(b) (6)@ironnetcybersecurity.com>

Tue, Jun 23, 2020 at 3:42 PM

To: FedRAMP <info@fedramp.gov>

Cc: (b) (6)@gsa.gov, (b) (6)@gsa.gov, (b) (6)@gsa.gov, john.hamilton@gsa.gov, (b) (6)

<(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>

Hi (b) (6)

Please find attached the signed RAR Evaluation template. It includes our responses and comments.

If you need any additional information, please do not hesitate to contact me.

Best regards,

(b) (6)

Cell: (b) (6)

Email: (b) (6)@ironnetcybersecurity.com

IronNet Cybersecurity Inc.

Governance, Risk and Compliance.

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

**IronNet CSP RAR Evaluation Template Final - 06232020 (signed).pdf**

106K

CSP Readiness Assessment Report (RAR) Evaluation

FedRAMP Review for:

IronNet Cloud w/FedRAMP (IronDefense / IronDome)

RAR Date:

05/15/2020

Ver.

1

System Categorization: Moderate

FedRAMP Evaluation Date:

6/24/20

Deployment Model: Private

Signed?

Yes

Service Model: SaaS

Recommended by 3PAO? Yes

3PAO Name: Kratos

Section A: Executive Summary

IronNet Cybersecurity, Inc. has completed the below Readiness Assessment Report (RAR) Self Assessment for the Cloud Service Offering (CSO) named IronNet Cloud w/FedRAMP (IronDefense / IronDome). This RAR Self-Assessment was completed concurrently with the RAR Evaluation performed by our Third Party Assessment Organization (3PAO). IronNet Cybersecurity IronNet Cloud w/FedRAMP (IronDefense / IronDome) is FedRAMP Ready.

SIGNED: _____

DATE: _____

(b) (6)

Ironnet Cybersecurity, Inc.

Section B: RAR Attestation/Executive Summary

#	Description	Free of Gaps/	Comments
1	Do the Readiness Assessment Activities within the Attestation section provide the date(s) and location(s) of the Readiness Assessment and a description of the 3PAO's activities?	Ok	Yes the assessment dates were from April 14th 2020 through May 15th 2020 and conducted on site (virtual) with Ironnet personnel normally residing at offices in Fulton MD. A full description of the 3PAO's activities are also included in the Readiness Assessment Activities section of the RAR.
2	Does the Executive Summary provide an adequate description of the system?	Ok	Yes the Executive Summary provides an adequate description of the IronNet Cloud system.
3	Does the Executive Summary provide an adequate overview of information/findings provided in Sections 4.1, 4.2, and 4.3, including notable strengths and other areas for consideration?	Ok	<p>Yes the Executive Summary provides an adequate overview to include strengths:</p> <ul style="list-style-type: none"> - Strong leadership and commitment to the FedRAMP program - Mature well defined and comprehensive configuration management using defined AWS components to deploy the SaaS services. Inheriting services from AWS GovCloud provides a comprehensive baseline configuration. <p>The Executive Summary also identified IronNet Cloud as not clearly defining customer responsibilities within their SSP and associated Customer Responsibility Matrix within Attachment 9 but will be finalized approved and signed within 90 days of receiving FedRAMP Ready status and before the formal FedRAMP assessment has begun.</p> <p>One item of note in the Executive Summary is a reference to the Sumo Logic Fed environment on page iv that appears to be a typo.</p>

Section C: CSP System Information (addresses RAR Section 3)

#	Description	Free of Gaps/	Comments
---	-------------	---------------	----------

1	Is the CSP system information within Table 3-1 complete? (§3.0)	Ok	Yes all system information provided in Table 3-1 is complete and accurate.
2	Are the relationships to other CSPs (Table 3-2) clearly defined, explained, and adequate?	Ok	The relationships in the leveraged FedRAMP Authorizations table are clearly defined and explained. However there is one service listed that is not leveraged by IronCloud; ElasticSearch. Also although the following 7 services leveraged by IronCloud were listed in the Figure 1: IronNet Authorization Boundary: NLB EFS Elastic IP Transit Gateway ELB Application Load Balancer and AWS Cert Manager. The first 6 were not included in Table 3-1 since they are considered part of EC2 Services and the last one "AWS Cert Manager" should be included in the Table.
3	Are the leveraged services (Table 3-3) clearly defined, explained and adequate? (§3.1)	Ok	Yes the leveraged services in the External Systems and Services table are clearly defined explained and adequate.
4	Has the RAR indicated that the 3PAO has performed a full validation of the authorization boundary? (§3.2)	Ok	Yes section 3.1 of the RAR indicates that the 3PAO has performed a full validation of the authorization boundary.
6	Has the RAR indicated and described any boundary exclusions? (§3.2.2)	Ok	Non-Applicable. The RAR does not indicate nor describe any boundary exclusions. All AWS and external services that are connected to IronCloud are listed.
5	In addition to a boundary diagram, has the RAR provided a written description that clearly and accurately describes the authorization boundary? (§3.2.1)	Ok	Yes the written description of the boundary diagram is clear and accurate. However there is an incorrect statement on page 7 regarding the Bind server in the Security Tools VPC. The correct description should read "IronDefense uses Route 53 for internal certificate validation only. All other DNS traffic is routed using DNSSEC via the Bind Server within the Security Tools VPC." Also on page 6 the seven components of IronCloud each within their own VPC is unclear. VPC #6 is "Compliance VPC" and #7 is "IronDefense VPC". The log data of changes is backhauled to the Logging AWS Account bucket.
7	In addition to the data flow diagrams, has the RAR provided a written description that adequately identifies and delineates the data flows (i.e., including how data enters and exits a system)? (§3.2.3)	Ok	Yes the RAR provides a written description that adequately identifies and delineates the data flows
8	Does the RAR demonstrate solid separation measures used by the CSP? (§3.3)	Ok	Yes the RAR demonstrates solid separation measures used by IronNet between the system and interconnected systems. (Page 19). In additionally describes the isolation in inner layers of IronDefense as orchestrated by Kubernetes.
9	Are the system interconnections and TIC capability clearly documented? (§3.4)	Ok	Yes system interconnections are clearly documented. In regard to TIC all external communications go thru managed interfaces which comply with TIC requirements.

Section D: Capability Readiness (addresses RAR Section 4.1)

#	Description	Free of Gaps/	Comments
1	Does the RAR state that all Federal Mandates are met? (§4.1)	Ok	Yes the RAR in the FedRAMP Mandates table 4-1 on page 22 states that IronCloud is compliant with all Federal Mandates.

2	Are FIPS 140-2 Validated or NSA Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? (§4.1, #1)	Ok	Yes IronCloud uses end-to-end NIST approved cryptographic modules.
3	Can the system fully support user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials? (§4.1, #2)	Ok	Yes IronCloud fully supports user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) using SAML 2.0.
4	Is the system operating at the minimum eAuth level for its FIPS-199 designated level of operation (Level 3 for Moderate, Level 4 for High)? (§4.1, #3)	Ok	Yes IronCloud is operating at the minimum eAuth level of MODERATE in accordance with FIPS-199.
5	Does the CSP have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? (§4.1, #4)	Ok	Yes IronNet remediation timelines fall within those parameters.
6	Does the CSP and system meet Federal Records Management Requirements, including the ability to support record holdings, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? (§4.1, #5)	Ok	IronCloud does not function as a system of record for a federal or government agency. Any information that may be contained in the system is an incidental copy of information originally retained by the agency itself.

Section E: Capability Readiness (addresses RAR Section 4.2)			
#	Description	Free of Gaps/	Comments
1	Does RAR Table 4-2 indicate that only Federally approved cryptographic modules are used consistently (SC-13)? (§4.2.1)	Ok	Yes the cryptographic modules (Table 4-2) indicate that Data at Rest Data in Transmission Remote Access Authentication and Digital Signatures all use FIPS 140.2 cryptographic modules.
2	Does the RAR indicate that all transport layer protocols are identified? (§4.2.2)	Ok	Yes the RAR indicates in the Transport Layer Security (table 4-3) that all transport layer protocols are identified and are at minimum TLS v1.2
3	Does RAR Table 4-4 sufficiently describe identification and authentication, authorization, and access controls? (§4.2.3)	Ok	Yes the RAR sufficiently describes identification and authentication authorization and access controls. This is depicted in table 4-4 by the use of PIV/CAC MFA using Google Cloud Identity and SSH access to EC2 instances which require either credentials or access key generated from the EC2 using a private key.
4	Does the RAR show the system has consistent audit, alerting, malware, and incident response controls in place? (§4.2.4)	Ok	Yes the RAR shows that IronCloud has consistent audit alerting malware and incident response controls in place. It shows that Anti-Virus Sophos and other tools can alert and feed Splunk in case of malicious activities.

5	Does the RAR indicate consistent contingency planning and disaster recovery controls in place? (§4.2.5)	Ok	Yes the RAR indicates that IronCloud has the ability to recover to previous known state in case of major Disaster Recovery/Continuity of Business event.
6	Does the CSP demonstrate consistent configuration and risk management controls? Specifically, are authenticated scans performed monthly on OS/ Infrastructure and Web and Database applications, as applicable? Are vulnerabilities remediated within the required timeframes? (§4.2.6)	Ok	<p>Yes IronNet has demonstrated consistent configuration and risk management controls. IronNet runs authenticated scans on all entities/assets in the Authorized boundary. This includes the OS Infrastructure IronVue (web- interface) and CITUS cluster databases. A typographical error in the RAR was identified where "Trustwave" is referenced on pages 28 29 37 as an integrity monitoring tool and should be replaced by AIDE a native function of RHEL7 to perform file integrity checking within the environment.</p> <p>However the remediation timeline is incorrect in the RAR report on page 40. Per IronNet policy related to remediation timeframe all HIGH severity vulnerabilities must be remedied within 30 days MODERATE 90 days and LOW 120 days.</p>
7	Does the RAR illustrate that the CSP has consistent data center security? (§4.2.7)	Ok	Yes the RAR illustrates that this control is provided by AWS GovCloud. AWS obtained JAB P-ATO on June 21 2006 under unique identifier F1603047866.
8	Does the RAR show that the CSP has a complete set of policies and procedures? (§4.2.8)	Ok	Yes the RAR shows that IronNet has a complete set of policies and procedures. However the final matured policies and procedures will include all required Moderate controls and enhancements within 90 days of receiving FedRAMP Ready status.
9	Does the RAR indicate that the CSP has adequate security awareness and role-based training? (§4.2.8)	Ok	Yes the RAR indicates that the CSP has adequate security awareness and role-based training which is initially provided by the CIO/CISO during the onboarding process as well as mandatory annual refresher training via Adobe Captivate Prime Learning Management System (LMS).

Section F: Additional Capability Information (addresses RAR Section 4.3)

#	Description	Free of Gaps/	Comments
1	Does the RAR indicate that the CSP is adequately staffed? (§4.3.1)	Ok	Yes the RAR indicates that IronNet is adequately staffed to support a company of approximately 303 employees in the entire company.
2	Does the RAR indicate a mature Change Management Capability? (§4.3.2)	Ok	Yes the RAR indicates that IronNet has a mature Change Management capability that is internally implemented by CAB (Change Management Board) processes.
3	Does the RAR show that CSP vendor dependencies and related agreements are adequately maintained? (§4.3.3)	Ok	Yes the RAR provides IronNet's vendor dependencies in the table 4 -15 on page 46-47.
4	Does the RAR indicate that the CSP has adequate Continuous Monitoring? (§4.3.4)	Ok	Yes the RAR indicates that IronNet has adequate Continuous Monitoring that leverages vulnerability and compliance checks using tools such as Nessus and feeds the results into a POA&M using Xacta360.
5	Does the RAR document the SSP maturity level? (§4.3.5)	Ok	Yes the RAR documents that IronNet has a SSP that is more than 50% developed. IronNet Could for FedRAMP SSP will be finalized and signed by CIO/CISO within 90 days of receiving FedRAMP Ready Status and before the formal FedRAMP assessment has begun.

v 17

Section G: Additional Comments



info fedramp <info@gsa.gov>

RE: [EXTERNAL] Re: [EXTERNAL] Re: IronNet RAR Evaluation Form - Signed

1 message

(b) (6) <(b) (6)@kratosdefense.com> Tue, Jun 30, 2020 at 10:49 AM
 To: (b) (6)@gsa.gov
 Cc: (b) (6)@ironnetcybersecurity.com <(b) (6)@ironnetcybersecurity.com>, (b) (6)@gsa.gov
 (b) (6)@gsa.gov, (b) (6)@gsa.gov <bridget.dorward@gsa.gov>, (b) (6)@gsa.gov
 <(b) (6)@gsa.gov>, (b) (6)@gsa.gov (b) (6)@gsa.gov, (b) (6)@gsa.gov
 <(b) (6)@gsa.gov>, john.hamilton@gsa.gov <john.hamilton@gsa.gov>, (b) (6)@ironnetcybersecurity.com
 <(b) (6)@ironnetcybersecurity.com>, (b) (6)@ironnetcybersecurity.com
 <(b) (6)@ironnetcybersecurity.com>, (b) (6)@ironnetcybersecurity.com
 <(b) (6)@ironnetcybersecurity.com>, info@fedramp.gov <info@fedramp.gov>

Thank you sir!

Sincerely, (b) (6)

Kratos | Chandler, AZ | TTS-Cyber Principal Security Consultant

C: (b) (6) | www.kratosdefense.com**KRATOS**

From: (b) (6) QQ-C [mailto:(b) (6)@gsa.gov]
Sent: June 30, 2020 7:48 AM
To: (b) (6)
Cc: (b) (6); (b) (6)@gsa.gov; (b) (6)@gsa.gov; (b) (6)@gsa.gov;
 (b) (6)@gsa.gov; (b) (6)@gsa.gov; john.hamilton@gsa.gov; (b) (6)@
 ironnetcybersecurity.com; (b) (6)@ironnetcybersecurity.com; (b) (6)@
 ironnetcybersecurity.com; info@fedramp.gov
Subject: Re: [EXTERNAL] Re: [EXTERNAL] Re: IronNet RAR Evaluation Form - Signed

Hi (b) (6)

I just forwarded the meeting invite for 11:30am this morning.

Best,

(b) (6)

On Tue, Jun 30, 2020 at 10:44 AM (b) (6) <(b) (6)@kratosdefense.com> wrote:

All, did this meeting get scheduled?

Sincerely, (b) (6)

Kratos | Chandler, AZ | TTS-Cyber Principal Security Consultant

C: (b) (6) | www.kratosdefense.com

KRATOS

From: (b) (6) [mailto:(b) (6)@ironnetcybersecurity.com]

Sent: June 26, 2020 7:44 PM

To: (b) (6) - Q-C
(b) (6) - QQC-C; (b) (6) - QQC; (b) (6) - QQC-C; (b) (6) - QQC-C;
(b) (6) - QQC-C; William Hamilton - QQC; (b) (6); (b) (6); (b) (6); FedRAMP;
(b) (6)

Subject: Re: [EXTERNAL] Re: [EXTERNAL] Re: IronNet RAR Evaluation Form - Signed

(b) (6)

That would be great....thanks for setting this up. See you then.

Warmest Regards,

(b) (6)

(b) (6), (b) (6)
Chief Information and Security Officer (CIO/CISO)

IronNet Cybersecurity

8135 Maple Lawn Blvd, Suite 455

Fulton, MD 20759

Cell: (b) (6)

(b) (6)@ironnetcybersecurity.com

On Fri, Jun 26, 2020 at 6:03 PM (b) (6) - QQC-C <(b) (6)@gsa.gov> wrote:

Hi (b) (6)

I'm happy to set up a call with our team next week. Are you available on Tuesday, 6/30 at 11:30am ET?

I can send an invite in the meantime.

Best,

(b) (6)

On Thu, Jun 25, 2020 at 2:39 PM (b) (6) <(b) (6)@ironnetcybersecurity.com> wrote:

Great, thanks so much (b) (6)

Nice to meet you (b) (6).

We are trying to explore options and strategize on the best way to approach a JAB Path. We have successfully completed our RAR Real Time meeting with the Agency Team on this thread, and in all honesty thought there was one path for FedRAMP Readiness to accommodate both Agency and JAB ATO paths. But yesterday it came to light, that is not exactly the case. I was hoping it would be possible to schedule a short call with one (or any) of you on the JAB side over the next few days to help guide us in the right direction. I am not sure if our Registration ID number is any help, but it is FR2020681957. Thanks for your time.

Hope all are well/safe.

Warmest Regards,

(b) (6)

(b) (6), (b) (6)
Chief Information and Security Officer (CIO/CISO)
IronNet Cybersecurity
8135 Maple Lawn Blvd, Suite 455
Fulton, MD 20759
Cell: (b) (6)
(b) (6)@ironnetcybersecurity.com

On Thu, Jun 25, 2020 at 2:25 PM (b) (6) - QQC-C <(b) (6)@gsa.gov> wrote:

Hi (b) (6)

Absolutely! It was a good discussion, and we're glad your team was so on the ball in answering questions!

I have copied members of our engagement team here, (b) (6). :) They are our engagement team, who will be able to discuss the process differences between the Agency and JAB paths in more detail than we got into yesterday.

Yours Truly,

(b) (6)

--

(b) (6) | FedRAMP Agency Reviewer

(b) (6) @gsa.gov

On Thu, Jun 25, 2020 at 1:54 PM (b) (6) <(b) (6) @ironnetcybersecurity.com> wrote:

(b) (6) (FedRAMP PMO Team),

Thanks for your time yesterday during our RAR Real Time Meeting. The team is busily working with our 3PAO (Kratos) to update and provide clarifying items in the RAR based on this session. Your insights and input were extremely valuable and we are planning to get this to you in the next few days.

Also during our session, you mentioned that it might be worth reaching out and talking to your JAB ATO SMEs for insights into that process. If you could point me in the right direction (email introduction or phone#) that would be greatly appreciated.

Warmest Regards,

(b) (6)

(b) (6), (b) (6)
Chief Information and Security Officer (CIO/CISO)
IronNet Cybersecurity
8135 Maple Lawn Blvd, Suite 455
Fulton, MD 20759
Cell: (b) (6)
(b) (6) @ironnetcybersecurity.com

On Wed, Jun 24, 2020 at 12:31 PM (b) (6) <(b) (6) @ironnetcybersecurity.com> wrote:

Hi (b) (6),

Looks like the attendance list got cut off in the Chat window...so attaching here from IronNet team.

Warmest Regards,

(b) (6)

(b) (6), (b) (6)

Chief Information and Security Officer (CIO/CISO)

IronNet Cybersecurity

8135 Maple Lawn Blvd, Suite 455

Fulton, MD 20759

Cell: (b) (6)

(b) (6) @ironnetcybersecurity.com

On Tue, Jun 23, 2020 at 3:42 PM (b) (6) <(b) (6) @ironnetcybersecurity.com> wrote:

Hi (b) (6)

Please find attached the signed RAR Evaluation template. It includes our responses and comments.

If you need any additional information, please do not hesitate to contact me.

Best regards,

(b) (6)

Cell: (b) (6)

Email: (b) (6) @ironnetcybersecurity.com

IronNet Cybersecurity Inc.

Governance, Risk and Compliance.

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

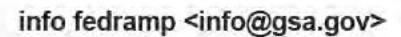
Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.



1 message

Wed, Jul 29, 2020 at 3:40 PM

(b) (6) -

https://mail.google.com/mail/b/ACtqoIJGnfsT2OtuzDgUGIHCE_D_vkMwOKP6STEOkiUrHxbLKF_/u/1/?ik=be8c5dee23&view=pt&search=all&permthid=thread... 1/2

--

John Hamilton
FedRAMP Program Manager of Security Operations
Technology Transformation Service | GSA
202.394.2812 | william.hamilton@gsa.gov

3 attachments



IronNet IronCloud FedRAMP Ready Approval Letter_072920.pdf
55K



IronNet IronCloud FedRAMP RAR Evaluation Report_072920.pdf
114K



FedRAMP Branding Guidance.pdf
615K



To: (b) (6)
President
IronNet Cybersecurity Inc.

7/29/2020

From: Ashley Mahan
FedRAMP Director
General Services Administration

Re: IronNet IronCloud FedRAMP Ready Approval - Agency Authorization Only

(b) (6) -

The FedRAMP PMO has completed evaluation of the IronNet IronCloud Readiness Assessment Report (RAR) provided by Kratos. Based on the outcome of the RAR evaluation, the cloud service offering (CSO) has been approved as FedRAMP Ready for Agency Authorization.

The FedRAMP PMO recognizes the CSO is still maturing documentation and capabilities such as updating the control family policies and procedures and system security plan (SSP). The FedRAMP PMO also recognizes that the CSO uses several third party providers and external services/systems lacking FedRAMP Authorization (at time of RAR) to support IronCloud (i.e., **Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, and WhoIs (API)**). Potential agency partners pursuing a FedRAMP Agency Authorization must accept risk for this use, since these services are not FedRAMP Authorized.

The FedRAMP PMO relies on you to ensure the security posture of your service offering protects federal agency data and for you to work closely with any potential agency(ies) to ensure they understand how their data will be protected in your environment. For example, in cases where several multi-factor authentication methods are provided by a service, cloud service providers (CSPs) must identify which methods of multi-factor access are/are not FIPS 140-2 validated, and encourage customers and partners to use methods that are FIPS validated.

We look forward to continue working with you as you pursue a FedRAMP Agency Authorization.

Please don't hesitate to reach out if you have any questions.

Sincerely,

Ashley Mahan
FedRAMP Director

Readiness Assessment Report (RAR) Evaluation Report

FR2020139614

FedRAMP Review for:	IronNet Cybersecurity inc., IronCloud	System Categorization:	Moderate
Recommendation:	FedRAMP Ready - Agency Auth. Only	Deployment Model:	Govt Only Comm.
RAR Date:	7/28/2020	Ver.	1.3
FedRAMP Evaluation Date:	7/28/2020	Service Model:	SaaS
Signed?	Yes	Recommended by 3PAO?	Yes
		3PAO Name:	Kratos

Section A: Executive Summary

The purpose of this report is to summarize the evaluation of Kratos' review of IronNet Cybersecurity Inc., IronCloud for consideration of the "FedRAMP Ready" designation. The evaluation of the Readiness Assessment Report (RAR) was conducted by the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO). The intended audiences for this report are agencies considering using the service offering, the Cloud Service Provider (CSP), and the Third Party Assessment Organization (3PAO).

Based on this RAR evaluation, the FedRAMP PMO has determined that this **Government Only Community** cloud service offering is FedRAMP Ready.

Agencies considering use of IronCloud should consider the following items of note:

1. Use of External Services Lacking FedRAMP Authorization: FedRAMP encourages use of FedRAMP Authorized services*, where possible. The RAR indicates that IronNet uses several third party providers and external services/systems lacking FedRAMP Authorization (at time of RAR) to support IronCloud (e.g., Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, and Whois [API]). The RAR describes external leveraged services and associated risks. The information provided in the RAR is intended to help agencies in determining the suitability of using the service based on each agency's risk tolerance. Agencies must understand that the use of services, that have not been FedRAMP Authorized, represent unknown risk and have not been validated by a 3PAO. Agencies must understand how their data is interacting with such services, and must assess and accept risk for the use of these external services, especially those services that provide critical security functionality. Agencies are encouraged to engage the CSP about questions concerning the use of the external services and may involve the FedRAMP PMO in such discussions, as desired.

2. Policies and Procedures: The CSP has a complete set of policies and procedures, but the 3PAO notes that some of the documents have some deficiencies that are being updated.

CSP Action: The policies and procedures should be updated and finalized prior to the initial full assessment.

3. SSP Completion: The SSP is 50% developed with an "overall operational maturity sufficient to satisfy FedRAMP requirements".

CSP Action: The SSP should be finalized prior to the initial full assessment.

4. Not applicable and Alternative Implementation controls: 8 controls are designated as N/A and 5 controls are designated as alternative implementations.

3PAO Action: These controls should be fully validated during the initial full assessment.

As part of risk-based authorization and use decisions, agencies are reminded to also review associated leveraged service authorization package(s), such as for the underlying Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), for full awareness of risks associated with using a cloud service.

*Note: Under most circumstances, the use of external services that lack FedRAMP Agency Authorization or Joint Authorization Board (JAB) Provisional Authorization (P-ATO) is permitted only if you are pursuing Agency Authorization, and if the initial partnering agency accepts risk. The JAB requirements related to external services are much more stringent; if interested in pursuing a JAB P-ATO, please inquire to info@fedramp.gov if you use any external services other than those with a JAB P-ATO.

Key:

Concern = May require CSP Action for FRR or FR Authorization.

OK = No necessary action for FedRAMP Ready to be granted.

N/A = Not applicable for this service.

Section B: RAR Attestation Statement & Executive Summary

#	Description	OK/Concern	Comments
1	Do the Readiness Assessment Activities within the Attestation section provide the date(s) and location(s) of the Readiness Assessment and a description of the 3PAO's activities?	Ok	
2	Does the Executive Summary provide an adequate description of the system?	Ok	
3	Does the Executive Summary provide an adequate overview of information/findings provided in Sections 4.1, 4.2, and 4.3, including notable strengths and other areas for consideration?	Ok	
4	Has 3PAO adhered to the numbered list of instructions in Section 2.2?	Ok	

Section C: CSP System Information (addresses RAR Section 3)

#	Description	OK/Concern	Comments
1	Is the CSP system information within Table 3-1 complete? (Section 3.0)	Ok	

Readiness Assessment Report (RAR) Evaluation Report

FR2020139614

2	Has the RAR indicated that the 3PAO has performed a full validation of the authorization boundary? (Section 3.1)	Ok	
3	In addition to a boundary diagram, has the RAR provided a written description that clearly and accurately describes the authorization boundary? (Section 3.1)	Ok	
4	Are the leveraged services clearly defined, explained and adequate? (Section 3.2 Table 3-2)	Ok	<i>AWS GovCloud, Google Services (Google Cloud Platform Products and underlying Infrastructure)</i>
5	Are all external systems and services noted in adequate detail? (Section 3.3 Table 3-3)	Ok	<i>Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, and Whois (API)</i>
6	Are all APIs that are used to push, pull, or exchange data and information with external resources listed and described? (Section 3.4 Table 3-4)	Ok	
7	Are the system's TIC capabilities clearly documented? (Section 3.5)	Ok	
8	Has the RAR indicated that the 3PAO has performed a full validation of the Data Flow Diagram(s)? (Section 3.6)	Ok	
9	In addition to the data flow diagrams, has the RAR provided a written description that adequately identifies and delineates the data flows (i.e., including how data enters and exits a system)? (Section 3.6)	Ok	
10	Does the RAR demonstrate solid separation measures used by the CSP? (Section 3.7)	Ok	

Section D: Capability Readiness (addresses RAR Sections 4.1 and 4.2)

#	Description	OK/Concern	Comments
1	Does the RAR adequately address all Federal Mandates? (Table 4-1)	Ok	
2	Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? (Section 4.2.1 and Table 4-2)	Ok	
4	Does the system properly describe and clarify its adherence to current Digital Identity requirements for Identification, Authentication, and Access controls in accordance with NIST SP 800-63 r3? (Section 4.2.3 and Table 4-4)	Ok	
5	Does the RAR show the system has consistent audit, alerting, malware, and incident response controls in place? (Section 4.2.4 and Table 4-5)	Ok	
6	Does the RAR indicate consistent contingency planning and disaster recovery controls in place? (Section 4.2.5 and Table 4-6)	Ok	
7	Does the CSP demonstrate consistent configuration and risk management controls? Specifically, are authenticated scans performed monthly on OS/Infrastructure and Web and Database applications, as applicable? Are vulnerabilities remediated within the required timeframes? (Section 4.2.6 and Table 4-7)	Ok	

Readiness Assessment Report (RAR) Evaluation Report

FR2020139614

8	Does the RAR illustrate that the CSP has consistent data center security? (Section 4.2.7 and Table 4-8)	Ok	
9	Does the RAR indicate that the CSP has a complete set of policies and procedures? (Section 4.2.8 and Table 4-9)	Ok	<p><i>The CSP has a complete set of policies and procedures, but the 3PAO notes that some of the documents have some deficiencies. IronNet is working with a trusted advisor to update these documents and the 3PAO states that these will be "finalized, approved, and signed within 90 days of receiving FedRAMP Ready status and before the formal FedRAMP assessment has begun."</i></p> <p><i>CSP Action: The policies and procedures should be updated and finalized prior to the initial full assessment.</i></p>
10	Does the RAR indicate that the CSP has adequate security awareness and role-based training? (Section 4.2.8 and Table 4-11)	Ok	

Section E: Additional Capability Information (addresses RAR Section 4.3)

#	Description	OK/Concern	Comments
1	Does the RAR indicate that the CSP is adequately staffed? (Section 4.3.1 and Table 4-12)	Ok	
2	Does the RAR indicate a mature Change Management Capability? (Section 4.3.2 and Table 4-13)	Ok	
3	Does the RAR show that CSP vendor dependencies and related agreements are adequately maintained? (Section 4.3.3 and Tables 4-14, 4-15, and 4-16)	Ok	
4	Does the RAR indicate that the CSP has adequate Continuous Monitoring? (Section 4.3.4 and Tables 4-17 & 4-18)	Ok	
5	Does the RAR document the SSP maturity level? (Section 4.3.5 and Table 4-19)	Ok	<p><i>The SSP is 50% developed with an "overall operational maturity sufficient to satisfy FedRAMP requirements".</i></p> <p><i>CSP Action: The SSP should be finalized prior to the initial full assessment.</i></p>
6	Does RAR document all controls currently designated "Not Applicable"? (Section 4.3.5, Table 4-20)	Ok	<p><i>8 controls are currently designated as "N/A", but the 3PAO disagrees with AC-19(5), PS-3(3), SC-15, and SC-18.</i></p> <p><i>3PAO Action: Please validate the status of these controls during the initial full assessment.</i></p>
7	Does RAR document all controls currently designated "Alternative Implementation"? (Section 4.3.5, Table 4-21)	Ok	<p><i>5 controls have alternative implementations, but the 3PAO disagrees with AC-19, CP-8, CP-8(1), and CP-8(2).</i></p> <p><i>3PAO Action: Please validate the status of these controls prior to the initial full assessment.</i></p>

v2.4

Section F: Additional Comments



FedRAMP

BRANDING GUIDANCE

February | 2018



FedRAMP

FedRAMP BRANDING GUIDANCE

Executive Summary

This document provides guidelines on the use of the FedRAMP name and logo on all FedRAMP marketing and collateral materials. General guidelines are provided first, followed by more specific guidelines for the two major uses of the FedRAMP mark:

- Designation of FedRAMP 3PAO accreditation
- FedRAMP Compliance

FedRAMP BRANDING GUIDANCE

Document Revision History

DATE	DESCRIPTION	AUTHOR
12/01/2012	Original Release	FedRAMP PMO
11/17/2014	Updated branding guidance to highlight proper use of new FedRAMP logo. Removed specific logos for 3PAOs or types of authorizations.	FedRAMP PMO
06/06/2017	Updated branding guidance to highlight proper use of new FedRAMP logo, color palette, fonts and icons.	FedRAMP PMO

FedRAMP BRANDING GUIDANCE

TABLE OF CONTENTS

Executive Summary.....	1
Document Revision History	2
FedRAMP Overview	4
General Guidelines.....	5
Color Palette	6
Logo Usage.....	7
Improper Logo Usage	7
Optional Uses of FedRAMP Logo.....	8
Typography	9
PowerPoint Template Style and Usage	10
Icon Style and Usage.....	10
FedRAMP Logo Review Policy	11
FedRAMP in Promotional Materials.....	12
Third Party Assessment Organization (3PAO) Use of FedRAMP Logo	13
Cloud Service Provider (CSP) Use of FedRAMP Logo	14

FedRAMP BRANDING GUIDANCE

FedRAMP Overview

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.

The objective of FedRAMP is threefold:

- Ensure that information systems/services used government-wide have adequate information security;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for federal agencies.

FedRAMP BRANDING GUIDANCE

General Guidelines

1. The FedRAMP logo refers to the FedRAMP name and FedRAMP approved logo detailed in this document.
2. The FedRAMP PMO will authorize an entity's ability to use the FedRAMP logo. The authorization will detail the specific circumstance(s) when an organization can use the FedRAMP logo.
3. The FedRAMP logo may never be used in any manner that would imply government endorsement of a company, its products, or its services. Neither the logo nor the FedRAMP name may be used in any other company name, product name, service name, domain name, or website title.
4. The logo may not be altered, cut apart, separated, or otherwise distorted in perspective or appearance.
5. The logo may never be used in a manner that would disparage FedRAMP or any government body.
6. Abbreviation of the Federal Risk Authorization Management Program must always appear as FedRAMP.
7. Authorized organizations are responsible for the proper use of the FedRAMP logo as outlined in this document. This includes but is not limited to the use by any representatives, such as advertising agencies, system integrators, resellers, partners, etc.

FedRAMP BRANDING GUIDANCE

Color Palette

If multicolor printing is available, please use the color scheme below.

Primary Color Palette



CMYK:
100/84/41/37

RGB:
17/46/81



CMYK:
5/100/78/0

RGB:
227/28/61



CMYK:
72/66/65/73

RGB:
33/33/33



CMYK:
66/55/45/20

RGB:
91/97/107



CMYK:
33/26/23/0

RGB:
174/176/181

Secondary Color Palette



CMYK:
10/0/2/0

RGB:
225/243/248



CMYK:
36/0/2/0

RGB:
155/218/241



CMYK:
69/0/5/0

RGB:
2/191/231



CMYK:
75/16/8/0

RGB:
0/166/210



CMYK:
91/54/20/3

RGB:
4/107/153



CMYK:
95/74/14/2

RGB:
31/84/147



CMYK:
13/100/99/3

RGB:
205/32/38



CMYK:
26/100/99/24

RGB:
152/27/30

Gradient



Secondary Blue

CMYK:
95/74/14/2

RGB:
31/84/147



Primary Blue

CMYK:
100/84/41/37

RGB:
17/46/81



FedRAMP

Logo Text



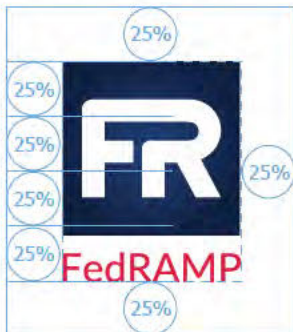
Primary Red

CMYK:
5/100/78/0

RGB:
227/28/61

FedRAMP BRANDING GUIDANCE

Logo Usage



Clear Space

We require the minimum amount of clear space to be equal to .25% of the height of the logo you use. No other graphic elements, such as text or images, can appear in this area. We require this clear space since the Promotional Logo frequently appears within materials using complex imagery, such as other logos, graphic devices, and text.



Grey-Scale Printing

If gray-scale printing is used, the logo must be printed using the color scheme below.

Gradient



Secondary Blue

CMYK: 0/0/0/85
RGB: 0/50/98

Primary Blue

CMYK: 0/0/0/100
RGB: 0/31/71

Logo Text



Primary Red

CMYK: 33/26/23/0
RGB: 174/176/181

Improper Logo Usage

Adhering to these guidelines is an integral part of creating a successful, memorable brand. Proper usage of the logo must be exercised in order to align all branded products. Do not alter the logo in any way. Here are some common mistakes.



FedRAMP

Cropping elements



FedRAMP

Disrupting the clear space



FedRAMP

Distorting the shape



FedRAMP

Disrupting the orientation



FedRAMP

Causing elements to overlap



Separating the elements

FedRAMP BRANDING GUIDANCE

Optional Uses of FedRAMP Logo

The FedRAMP logo can use the text “FedRAMP” or stand alone as mark in the following ways:

Official approved
FedRAMP logo



FedRAMP

Additional logo and color logo usage options:



FedRAMP



FedRAMP



FedRAMP

No text option



Logo usage on dark background



FedRAMP



FedRAMP



FedRAMP



FedRAMP



FedRAMP

All logos are available for download, please select an individual logo above or **click here** for all of them.

FedRAMP BRANDING GUIDANCE

Typography

When designing an original product that reflects the FedRAMP brand, this primary set of fonts should be used. These typefaces offer variety, while adhering to the elements established in the FedRAMP brand.

HEADER | Gill Sans

Gill Sans Light
Gill Sans Light Italic
Gill Sans Regular
Gill Sans Semi Bold
Gill Sans Semi Bold Italic

Gill Sans Bold
Gill Sans Bold Italic
Gill Sans Ultra Bold

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj
Kk Ll Mm Nn Oo Pp Rr Ss Tt
Uu Vv Ww Xx Yy Zz
1234567890 !?(){}|;:

BODY TEXT | Calibri

Calibri Regular
Calibri Italic
Calibri Bold
Calibri Bold Italic

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj
Kk Ll Mm Nn Oo Pp Rr Ss Tt
Uu Vv Ww Xx Yy Zz
1234567890 !?(){}|;:

MAIN HEADER

Sub-Header

Sub Sub-Header

Ipsae peliqua: Spelige ndaerep edigent asped mod et hitatia epedit eaque plique por aut vendeli quationseria ne cone nonseque omniat valoris serestio dit, ommo corro culpa sim fugiani musantor sa vel moluptati tem es voleste culpari tatur, si doluptatur raturecti sed modi autem ra nimi, ilignihil molecte moditatibus eumquia:

- Aaut molendi as denisqui nobis etur sectoruptiam.
- Soloreror sit, cus et que parum a commolu ptasimus et dempel iurerrumquis inveni.
- Modis iliquo odicte sam quati ut volorectur siminverupti a dent prore rest, voluptat aut opti.


Inci occus consequi bearum et im qui totatempor mi, volupta tibus aut enemqui aspientis dusae. Itae dunt labo. Ur, expe pro ducit, ut est, officid quia coris dendaep udicius evellorerero doluptam vel iunt et asperum volorepro.

1. Voluptate od ex eario. Itatur, quiae natus sit mod evelit omnisquia id quia dolescia dis
2. Doluptibus, id ullaccusam iunt ernatur sanis voluptaquia sunt expe nus eos mod quatem

Il is moditat atesse perchitis eatem re, ex erspiet dellorem quis et ma id ut pa sim apelibu sanditin nos nisinve rferibus, con reium solupturero occaborehent perit rempeliscid ere perum imus, omnitis aut eos sent.

FedRAMP BRANDING GUIDANCE

PowerPoint Template Style and Usage



The diagram shows a PowerPoint slide layout. At the top left is the 'FR' logo. To its right is the 'SLIDE TITLE' placeholder. Below the title is a 'Sub-header' placeholder. Below the sub-header is a bulleted list item. Callout lines point from these elements to their respective style specifications on the right.

Slide Header:


Gill Sans Bold
Size: 18pt
Color: Primary blue
C 100 | M 84 | Y 41 | K 37

Body Text Header:


Gill Sans Semi - Bold
Size: 16pt
Color: Primary red
C 5 | M 100 | Y 78 | K 0

Body Text:

Calibri Regular
Size: 14pt
Color: Primary dark gray
C 72 | M 66 | Y 65 | K 73



CMYK:
100/84/41/37
RGB:
17/46/81



CMYK:
5/100/78/0
RGB:
227/28/61

Icon Style and Usage



Primary Icon Style

Please use this primary icon style for your graphic needs:

Background:

Secondary Blue
C 69 | M 0 | Y 5 | K 0

Elements:

White
C 0 | M 0 | Y 0 | K 0

Secondary Icon Style



Secondary Blue
C 69 | M 0 | Y 5 | K 0



Background:

Primary Blue
C 100 | M 87 | Y 34 | K 25

Elements:

Secondary Blue
C 69 | M 0 | Y 5 | K 0



Background:

Primary Blue
C 100 | M 84 | Y 41 | K 37

Elements:

White
C 0 | M 0 | Y 0 | K 0



Background:

Lighter Gray
C 66 | M 55 | Y 45 | K 20

FedRAMP BRANDING GUIDANCE

FedRAMP Logo Review Policy

- Use of the FedRAMP logo in conjunction with qualified products or services (i.e. an approved 3PAO) does not require approval.
- The FedRAMP PMO must approve any major educational or promotional campaigns that feature the FedRAMP logo prior to use. The submitted materials will be reviewed for consistency with these guidelines within two (2) weeks of receipt of the materials. Materials should be submitted to the FedRAMP Director at info@fedramp.gov with the following in the subject line: “FedRAMP Branding Review.”

Logo Violations

The FedRAMP PMO actively monitors proper use of the FedRAMP logo. This includes but is not limited to the use by any representatives such as advertising agencies, system integrators, resellers, partners, etc. The following explains the general course of action for addressing logo violations:

1. Anyone who misuses the logo will be contacted in writing or by telephone.
2. The FedRAMP Program Management Office will provide a distinct timeframe to correct the error(s). The timeframe will be dependent upon the medium in which the violation appeared and the severity of the violation.
3. Follow-up will be conducted to ensure that the error(s) has been corrected.

Failure to make the required changes may result in termination of a stakeholder’s participation in FedRAMP and/or legal action.

Questions about Using the FedRAMP Logo

If you have questions regarding the use the FedRAMP logo, please contact the FedRAMP PMO at info@fedramp.gov.

FedRAMP BRANDING GUIDANCE

FedRAMP in Promotional Materials

This section outlines the messages that FedRAMP believes are important to convey regarding the benefits of the program. The government incorporates three messages into its materials and recommends those meeting the guidelines outlined in this document do the same, to the extent possible. The messages are:

The goal of FedRAMP is to:

- Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations
- Increase confidence in the security of cloud solutions
- Achieve consistent security authorizations using a baseline set of agreed upon standards for cloud solution
- Ensure consistent application of existing security practices
- Increase confidence in security assessments
- Increase automation and near real-time data for continuous monitoring

Major benefits of FedRAMP

- Increases re-use of existing security assessments across agencies
- Saves significant cost, time and resources – do once, use many times
- Improves real-time security visibility
- Provides a uniform approach to risk-based security management
- Enhances transparency between government and cloud service providers (CSPs)
- Improves the trustworthiness, reliability, consistency, and quality of the Federal security authorization process

FedRAMP BRANDING GUIDANCE

Third Party Assessment Organization (3PAO) Use of FedRAMP Logo

FedRAMP allows the use of the FedRAMP logo for FedRAMP accredited 3PAOs under the following conditions:

1. You must be a FedRAMP accredited 3PAO and maintain that accreditation in order to use the FedRAMP logo.
2. An accredited FedRAMP 3PAO can refer to themselves in the following ways:
 - Accredited FedRAMP 3PAO
 - Accredited FedRAMP Third Party Assessment Organization
 - FedRAMP 3PAO
 - FedRAMP Third Party Assessment Organization
3. An organization can use the official FedRAMP logo to designate themselves as an Accredited 3PAO.
4. FedRAMP accredited 3PAOs receive an official letter from the FedRAMP PMO designating their authorization to use the FedRAMP logo in the manner described above.

FedRAMP BRANDING GUIDANCE

Cloud Service Provider (CSP) Use of FedRAMP Logo

FedRAMP allows the use of the FedRAMP logo for CSPs that have met the FedRAMP requirements and are deemed FedRAMP compliant by the FedRAMP PMO. In order to use the FedRAMP logo, a CSP must have their completed security authorization package available for Federal Agency leveraging within the FedRAMP secure repository.

FedRAMP Compliant CSPs

1. A CSP with this level of authorization can refer to their product or service in the following ways:
 - Meet the FedRAMP security requirements
 - Utilized a FedRAMP accredited 3PAO
 - Granted an Authority to Operate by [Federal Agency(ies)].
2. The use of the official FedRAMP logo must clearly align with the product or service named within the assessment materials used to earn the Agency ATO.



info fedramp <info@gsa.gov>

Business Case Submission for IronNet Cloud for FedRAMP Connect

1 message

(b) (6) <**(b) (6)**@ironnetcybersecurity.com>

Fri, Nov 6, 2020 at 9:05 AM

To: FedRAMP <info@fedramp.gov>

Cc: **(b) (6)** <**(b) (6)**@ironnet.com>, **(b) (6)** <**(b) (6)**@ironnetcybersecurity.com>, **(b) (6)** <**(b) (6)**@ironnetcybersecurity.com>

FedRAMP Connect Team,

Please find enclosed our CSP Submission for this FedRAMP Connect cycle.

1. The JAB Prioritization Information Form
2. The Proof of Demand Worksheet

We appreciate your consideration, and look forward to hearing from you soon.

Warmest Regards,

(b) (6)**(b) (6)**, **(b) (6)**

Chief Information and Security Officer (CIO/CISO)

IronNet Cybersecurity



7900 Tysons One Place, Suite 400

McLean, VA 22102

Cell: **(b) (6)****(b) (6)**@ironnetcybersecurity.com

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

2 attachments **CSP_JAB_Prioritization-BCD-Worksheet.xlsx**
20K **CSP_JAB_Prioritization_Business_Case_Form (IronNet November 2020).pdf**
362K



FEDRAMP BUSINESS CASE

FOR JAB PRIORITIZATION

IronNet Cybersecurity

November 6, 2020

I. Cloud Service Provider (CSP) And Cloud Service Offering (CSO) Information

1.1 CSP Name: **IronNet Cybersecurity, Inc.**

1.2 System Name: **IronNet Cloud**

1.3 CSP Website: <https://www.ironnet.com/>

1.4 Two Points of Contact

(Name, Email, and Phone Number):

(b) (6),
(b) (6)@ironnet.com,
(b) (6),
(b) (6)@ironnet.com, (b) (6)

1.5 Cloud service Model:

- ☒ SaaS
☐ IaaS
☐ PaaS

1.6 Deployment Model:

- ☒ Public Cloud
☐ Government Only Cloud
☐ Fed Government Only Cloud
☐ DoD Cloud

1.7 FIPS 199 Impact Level:

- ☐ High
☒ Moderate
☐ Low

1.8 a Do you own your entire infrastructure? ☒ No ☐ Yes

1.8 b If no, what is the name of the JAB Authorized infrastructure you are using?

(If you are using an Agency Authorized infrastructure, you are not eligible for a JAB P-ATO.)

AWS GovCloud

1.9 Is the CSO FedRAMP Ready? ☐ No ☒ Yes

The CSO currently has the following certifications:

2. IronNet is ISO/IEC 27001:2013 Certified and SRI Quality System is our Registrar through ANAB (Certifying body), our certificate #020111 is valid through November 12, 2020. We have successfully completed our 3-year unconditional renewal, pending final report due mid-November.

Besides the SOC2 Types I & II and the ISO/IEC 27001 listed above for the past three years, the CSP is also GDPR-Compliant since 2018. This consistent and independantly audited history of meeting Information Security Management Systems standards since 2017 demonstrates a proven track record of mature organizational processes.

The CSO aligns with National Cybersecurity Strategy, Sep 2018, Pillar I by providing network detection and response and collective defense capabilities to secure Federal Networks and Information, secure Critical Infrastructure, and combat Cybercrime and Improve Incident Reporting. IronNet in 2018 received two separate acceptances/approvals for the DHS Continuous Diagnostics & Monitoring Approved Products List (CDM APL) for IronDefense (IRO-0002-20180103) and IronDome (IRO-0004-20180405).

2. Brief Service Description:

In the space below, provide a brief description of your service and the value it would bring to the Federal Government. Questions this write-up should address include:

- 1) How does an agency use and experience you offering?
- 2) How is your CSO broadly applicable across the Federal Government?
- 3) Does your CSO provide a new and innovative service?
- 4) Why should the JAB authorize your service over similar offerings?

IronNet Cloud with FedRAMP (IronDefense / IronDome) provides a cloud-based network behavioral analytics platform for customers to detect network-based malicious traffic on all five stages of the cyber security kill chain: Reconnaissance, Access, C2, Action, and 'other'. (Note: The use of "other" in this context is used as a catch-all for items not classified in the cyber security kill chain. The other classification, allows the algorithms to process the kill chain for items unknown in class, or the other classification.)

IronDefense processes customer and agency metadata, network traffic for threat behavioral analytics, and integrated hunt algorithms to detect malicious threat traffic. IronDefense and IronDome combines capabilities to provide the industry's first collective defense solution that links industry peers, third-party suppliers, and other stakeholders into a joint defense infrastructure.

With the rise of cyber attacks during the COVID-19 pandemic and the resulting economic crisis, we need to better understand threats and work together, collectively, in order to stop them. Our federal critical infrastructure and the wealth of our country are at risk. State by state, and as a nation, identifying unknown threats and collaborating to defend against them in real-time are critical to our success. In other words, cybersecurity is national security and is applicable across our entire Federal Government. Consider our current situation:

- Nation-state adversaries and other major threat actors have their eye on American critical infrastructure and other key systems across the public and private sectors. In 2018, for example, the U.S. publicly accused Russia of conducting a two-year long coordinated campaign of cyber intrusions into the U.S. grid.

- Adversaries are seeking to take advantage of new vulnerabilities in the midst of the current pandemic.

Cybersecurity agencies from the U.K., Canada, and the U.S. recently attributed a campaign targeting pharmaceutical companies and academic institutions involved in COVID-19 vaccine development to APT29, a group widely believed to be operating on behalf of Russian intelligence services.

- New levels of remote working and learning are increasing vulnerabilities. The education sector has reported the highest percentage (61%) of enterprise malware attacks of all industries in the last 30 days, according to Microsoft Security Intelligence.

IronDefense / IronDome is the path to Collective Defense and how Federal Agencies can gain the knowledge needed and the ability to collaborate at the speed of attack.

What makes Collective Defense such a powerful tool is the cyber threat sharing platform that allows participating organizations to become aware of and thwart cyber attacks targeting similar organizations. By sharing cyber anomalies in real time across a community of peers and within situational context, companies can identify attackers earlier in the attack cycle (that is, the cyber kill chain) when many of their methods fall below the threshold of detection. In other words, behavioral analytics can detect "unknown unknowns," making this new approach to cybersecurity a stronger defense approach than signature-based analytics often used in Network Traffic Analysis (NTA) solutions. Collective Defense sharing complements Information Security and Analysis (ISAC) groups and Threat Intelligence Platforms (TIPs).

FedRAMP Business Case: Proof of Demand Worksheet

In order to accurately evaluate demand, the FedRAMP PMO has developed this excel

Instructions:

- 1) Complete each relevant tab with the required information. We will not contact any of the refer
- 2) Do NOT PDF this excel. Save your completed excel worksheet as "[CSP's Name] Demand Works
- 3) Submit your completed excel worksheet to info@fedramp.gov WITH your JAB Prioritization Inf

el worksheet for CSPs to complete in order to show proof of 1)

rences provided without your knowledge and consent. If you have questions
heet [Submission Date]."
ormation Form.

Table 1: Proof of Demand from Current Federal Customers
Instructions: List all current Federal Agency customers of your business.

Existing Unique Federal Customers

Navy NAVSEA Defense Industrial Base Pilot

Army G2/TSMO Defense Industrial Base Pilot

--

[illegible]

Customers Worksheet

Customers Worksheet

(b) (6)

Program Owner Point of Contact Title

Director of International Programs

Senior Advisor for S&T and Innovation, ARMY G2

Program Owner	Point of Contact	E-mail
1.1.1.1		

(b) (6) @navy.mil

(b) (6) [REDACTED] .civ@mail.mil

or example, if an agency is using an on premise versio

Program Owner	Point of Contact	Phone Number

(b) (6)

on of your offering, or is using another offerin

Contract Officer	Point of Contact Name
[REDACTED]	[REDACTED]

(b) (6)

(b) (6) @quantum-intl.com

g, then they are not considered current demand in

[illegible]

Contract Officer Point of Contact E-mail

(b) (6) @bah.com

(b) (6) quantum-intl.com

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

[illegible]

(b) (6)

Government Contract Number

N00178-04-D-4024

W31P4Q-18-D-A003

[illegible]

our offering for this ATO, this would not be a current customer.

[illegible]

Table 2: Proof of Demand from Indirect Customers With
Instructions: List all CSP Customers with a FedRAMP ATO that use

Name of the FedRAMP-Authorized CSP Customer Using your Service:

<Example: ABC Government Cloud>

[illegible]

**orksheet
your service.**

FedRAMP CSP Point of Contact Name	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

<Example: Matt Goodrich>

FedRAMP CSP Point of Contact Title	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

<Example: FedRAMP Director>

[illegible]

FedRAMP CSP Point of Contact E-mail

<Example: matt@goodrich.com >

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

FedRAMP CSP Point of Contact Phone Number

<Example: 202-555-5555>

[illegible]

<Example: FR1234567891>

Number of FedRAMP ATOs issued for the FedRAMP CSO	
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	0
2020	0
2021	0
2022	0
2023	0
2024	0
2025	0
2026	0
2027	0
2028	0
2029	0
2030	0

<Example: 24>

Table 3: Proof of Demand from Current State, Local, Tribal, Territorial, Federal, and International Markets
Instructions: List all current State, Local, Tribal, Territorial, Federal, and International Markets

Existing Unique Customers

Lower Colorado River Authority TX

New York Power Authority

[illegible]

cal Tribal Territorial Federally Funded Research Cen
ederally Funded Research Centers (FFRDC), or Lab customers of yc
Jurisdiction/Type (i.e. State, Local, Tribal, Territorial, FFRDCs, or La

TX

NY

[illegible]

eters (FERDC) or Lab Customers W
our Cloud Service Offering being proposed to

Program Owner Point of Contact Name

(b) (6)

Worksheet

or JAB Prioritization.

[illegible]

Program	Owner	Point of Contact	E-mail
1	2	3	4

(b) (6) [REDACTED]@lcra.org

(b) (6) [REDACTED]@nypa.gov

[illegible]

[illegible]

[illegible]

Contract Officer Point of Contact E-mail

(b) (6)

[@LCRA.org](mailto:info@LCRA.org)

nypa.gov

[illegible]

[illegible]

[illegible]

Table 4: Proof of Potential
Instructions: List all Federal Agencies

Federal Agency Name
DIR
Golden Company - IC
ARMY ARCYBER
ARMY PEO STI
Air Force EITaaS
Air Force SIBR
Howard County (HCPSS)

tial Demand from Federal Agencies via RFI, RFP, or RFQ related

Name of RFI, RFP, or RFQ
Software Solutions Augmenting DIR-ISO-IMP-416
SIGHBURGER
RFQ Behavior Analytics
Cyber Trident Cyber Training, Readiness, Integration, Del
Enterprise IT as a Service
Small Business Innovation Phase II
Managed Security Services Solution

s, RFPS, and RFQs Work
to your cloud service that you ha

RFI, RFP, or RFQ Number
DIR-COPO-RFI-007
RFI-20-00091/BASE
Direct Request
Solicitation W900KK-20-R-0001
17-ITCC-044
J201-CS01
002.21.B5-IQII

1001
ive responded to in the last 18 mon

Contract Point of Contact Name	
(b) (6)	
	12
(b) (6)	

ths. The FedRAMP PMO reserves the right

Contract Point of Contact Title
Procurement Officer
Contracting Officer
Industry Engagement & Tech Assessment
PM CT2 – PdM CRT
Contracting Officer
Contracting Officer
Contracting Officer

Contract Point of Contact	E-mail

(b) (6) @dir.texas.gov

(b) (6) @tensleyconsulting.com

(b) (6) @mail.mil

fl.lst.pm-ltts@mail.mil

(b) (6) @us.af.mil

(b) (6) @hcnss.org

(b) (6) arxiv.org/abs/1607.04687

bmission for validation purposes.

Contract Point of Contact Phone Number	
NA	
(b) (6)	

Release Date	Submission Date
03/10/20	04/30/20
12/18/20	02/28/20
03/01/20	05/15/20
06/11/20	07/30/20
5/24/20	7/2/20
2/3/20	6/15/20
8/16/20	9/2/20



William Hamilton - QQC <william.hamilton@gsa.gov>

IronNet FedRAMP Real Time RAR Review Meeting

6 messages

(b) (6) - QQC-C (b) (6) @gsa.gov Thu, Jun 11, 2020 at 12:07 PM
 To: (b) (6) @ironnetcybersecurity.com, (b) (6) @castus.tv, (b) (6) @castus.tv, (b) (6) @kratosdefense.com
 Cc: (b) (6) - QQC-C (b) (6) @gsa.gov, (b) (6) - QQC-C (b) (6) @gsa.gov,
 William Hamilton - QQC <john.hamilton@gsa.gov>

Good afternoon IronNet team -

The FedRAMP PMO has begun the Readiness Assessment Report (RAR) for IronNet Cybersecurity Inc.-IronNet Cloud with FedRAMP. We would like to schedule a meeting with both of your teams to conduct a comprehensive, Real Time Review of your RAR. The intended outcome is to more efficiently resolve issues identified in the RAR and to have your 3PAO partner, Kratos, make agreed upon revisions to the RAR during the meeting. We would like to get a hold on all of our calendars for **Wednesday June 24th from 12pm EST to 4pm**. Coordinate amongst yourselves, then let me know if you are all available at that time. Attendance may be either in person at the GSA Building, or remote.

The agenda for this Real Time Review will be to go through the RAR from beginning to end, and address all questions and comments your reviewers have found along the way. As they are answered, the 3PAO will be able to make edits to the RAR in real time. To that end, please:

1. Ensure someone from the 3PAO team is ready to present the RAR to this group, both in person and on the Google Hangout that will be provided in the invite.
2. Ensure the Presenter keeps track changes on while editing the document.
3. Consider that any parties who wish to follow along with the edits plan on logging into Google Hangouts -- the link to which will be in the meeting invite.

At the end of the meeting the PMO and 3PAO will run through our comments, and the 3PAO will upload the track changes version of the RAR to OMB Max.

For both teams, please ensure you are familiar with the standard FedRAMP RAR Review process. I have attached the pertinent process document, for your reference

For the CSP team: Prior to the meeting, we need a member of the CSP team to complete and sign the attached "CSP RAR Evaluation Template v1.1" document, which is a self-assessment and attestation that CSP is aware that the 3PAO RAR submission is ready for FedRAMP PMO analysis and review. Once the RAR evaluation template is completed, please email info@fedramp.gov.

Thank you, we look forward to working further with you.

Yours Truly,

(b) (6)

(b) (6) | FedRAMP Agency Reviewer
 (b) (6) @gsa.gov

2 attachments

CSP RAR Evaluation Template v1.xlsx
 354K

FedRAMP RAR Review Process v1.1.pdf
 309K

(b) (6) - QQC-C (b) (6) @gsa.gov Thu, Jun 11, 2020 at 12:09 PM
 To: (b) (6) @ironnetcybersecurity.com, (b) (6) @castus.tv, (b) (6) @castus.tv, (b) (6) @kratosdefense.com
 Cc: (b) (6) - QQC-C (b) (6) @gsa.gov, (b) (6) - QQC-C (b) (6) @gsa.gov,
 William Hamilton - QQC <john.hamilton@gsa.gov>

Note -- Attendance will ONLY be remote, by Google Meet. We are not in the GSA office at this time.

Yours Truly,

(b) (6)

--

(b) (6) | FedRAMP Agency Reviewer
(b) (6) @gsa.gov

[Quoted text hidden]

(b) (6) <(b) (6)@kratosdefense.com> Thu, Jun 11, 2020 at 5:24 PM
To: (b) (6) @gsa.gov <(b) (6)@gsa.gov>, (b) (6) @ironnetcybersecurity.com
<(b) (6)@ironnetcybersecurity.com>, (b) (6)@castus.tv <(b) (6)@castus.tv>, (b) (6)@castus.tv <(b) (6)@castus.tv>
Cc: (b) (6) @gsa.gov <(b) (6)@gsa.gov>, (b) (6) @gsa.gov <(b) (6)@gsa.gov>, john.hamilton@gsa.gov <john.hamilton@gsa.gov>

Good afternoon (b) (6) and PMO team,

Is there flexibility in the single date provided, or can the FedRAMP PMO provide possible alternative dates that may work both for IronNet and the 3PAO?

Normally, I see the invites with a choice of possible dates, so that schedules can be accommodated. If this is not the case, the teams will have to make it work.

Just checking.

Sincerely, (b) (6)

Kratos | Chandler, AZ | TTS-Cyber Principal Security Consultant

C: (b) (6) | www.kratossecureinfo.com

KRATOS

[Quoted text hidden]

(b) (6) - QQC-C <(b) (6)@gsa.gov> Fri, Jun 12, 2020 at 10:15 AM
To: (b) (6) <(b) (6)@kratosdefense.com>
Cc: (b) (6) @ironnetcybersecurity.com <(b) (6)@ironnetcybersecurity.com>, (b) (6)@castus.tv <(b) (6)@castus.tv>, (b) (6)@castus.tv <nathan@castus.tv>, (b) (6) @gsa.gov <(b) (6)@gsa.gov>, (b) (6) @gsa.gov <(b) (6)@gsa.gov>, john.hamilton@gsa.gov <john.hamilton@gsa.gov>

Good morning (b) (6)

Because of the length of these meetings, and how many we hold, I'm sorry there isn't too much flexibility. It's why we generally only offer one time period. June 24th is the earliest possible, and the next available dates will be the week of July 6th. If you would prefer that week, let me know.

Yours Truly,

(b) (6)

--

(b) (6) | FedRAMP Agency Reviewer
(b) (6) @gsa.gov

[Quoted text hidden]

(b) (6) <(b) (6)@kratosdefense.com> Fri, Jun 12, 2020 at 10:47 AM
To: (b) (6)@gsa.gov <(b) (6)@gsa.gov>
Cc: (b) (6)@ironnetcybersecurity.com <(b) (6)@ironnetcybersecurity.com>, (b) (6)@castus.tv
<(b) (6)@castus.tv>, (b) (6)@castus.tv <(b) (6)@castus.tv>, (b) (6)@gsa.gov <(b) (6)@gsa.gov>,
(b) (6)@gsa.gov <(b) (6)@gsa.gov>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>

Thank you (b) (6) We will have to make it work.

[Quoted text hidden]

(b) (6) - QQC-C (b) (6)@gsa.gov Fri, Jun 12, 2020 at 11:58 AM
To: (b) (6) <(b) (6)@kratosdefense.com>
Cc: (b) (6)@ironnetcybersecurity.com <(b) (6)@ironnetcybersecurity.com>, (b) (6)@castus.tv
<(b) (6)@castus.tv>, (b) (6)@castus.tv <(b) (6)@castus.tv>, (b) (6)@gsa.gov <(b) (6)@gsa.gov>,
(b) (6)@gsa.gov <laurie.southernton@gsa.gov>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>

Groovy, then I will have the invite out momentarily.

Yours Truly,

(b) (6)

--

(b) (6) | FedRAMP Agency Reviewer
(b) (6) @gsa.gov

[Quoted text hidden]

CSP Readiness Assessment Rep**FedRAMP Review for:****RAR Date:****FedRAMP Evaluation Date:****Signed?****Ver.****Section A: Executive Summary**

<CSP NAME> has completed the below Readiness Assessment Report (RAR) Self Assessment. RAR Self-Assessment was completed concurrently with the RAR Evaluation performed by o document is our signed attestation to FedRAMP that <CSP NAME> <CSO NAME> is FedR/

SIGNED: _____ DATE: _____

Section B: RAR Attestation/Executive Summary

#	Description	Free of Gaps/ Missing Elements?
1	Do the Readiness Assessment Activities within the Attestation section provide the date(s) and location(s) of the Readiness Assessment and a description of the 3PAO's activities?	----
2	Does the Executive Summary provide an adequate description of the system?	----
3	Does the Executive Summary provide an adequate overview of information/findings provided in Sections 4.1, 4.2, and 4.3, including notable strengths and other areas for consideration?	----

Section C: CSP System Information (addresses RAR Section 3)

#	Description	Free of Gaps/ Missing Elements?
1	Is the CSP system information within Table 3-1 complete? (§3.0)	----
2	Are the relationships to other CSPs (Table 3-2) clearly defined, explained, and adequate?	----

3	Are the leveraged services (Table 3-3) clearly defined, explained and adequate? (§3.1)	----
4	Has the RAR indicated that the 3PAO has performed a full validation of the authorization boundary? (§3.2)	----
5	In addition to a boundary diagram, has the RAR provided a written description that clearly and accurately describes the authorization boundary? (§3.2.1)	----
6	Has the RAR indicated and described any boundary exclusions? (§3.2.2)	----
7	In addition to the data flow diagrams, has the RAR provided a written description that adequately identifies and delineates the data flows (i.e., including how data enters and exits a system)? (§3.2.3)	----
8	Does the RAR demonstrate solid separation measures used by the CSP? (§3.3)	----
9	Are the system interconnections and TIC capability clearly documented? (§3.4)	----

Section D: Capability Readiness (addresses RAR Section 4.1)

#	Description	Free of Gaps/ Missing Elements?
1	Does the RAR state that all Federal Mandates are met? (§4.1)	----
2	Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? (§4.1, #1)	----
3	Can the system fully support user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials? (§4.1, #2)	----
4	Is the system operating at the minimum eAuth level for its FIPS-199 designated level of operation (Level 3 for Moderate, Level 4 for High)? (§4.1, #3)	----
5	Does the CSP have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? (§4.1, #4)	----

6	Does the CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? (§4.1, #5)	----
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------

Section E: Capability Readiness (addresses RAR Section 4.2)

#	Description	Free of Gaps/ Missing Elements?
1	Does RAR Table 4-2 indicate that only Federally approved cryptographic modules are used consistently (SC-13)? (§4.2.1)	----
2	Does the RAR indicate that all transport layer protocols are identified? (§4.2.2)	----
3	Does RAR Table 4-4 sufficiently describe identification and authentication, authorization, and access controls? (§4.2.3)	----
4	Does the RAR show the system has consistent audit, alerting, malware, and incident response controls in place? (§4.2.4)	----
5	Does the RAR indicate consistent contingency planning and disaster recovery controls in place? (§4.2.5)	----
6	Does the CSP demonstrate consistent configuration and risk management controls? Specifically, are authenticated scans performed monthly on OS/	----
7	Does the RAR illustrate that the CSP has consistent data center security? (§4.2.7)	----
8	Does the RAR show that the CSP has a complete set of policies and procedures? (§4.2.8)	----
9	Does the RAR indicate that the CSP has adequate security awareness and role-based training? (§4.2.8)	----

Section F: Additional Capability Information (addresses RAR Section 4

#	Description	Free of Gaps/ Missing Elements?
1	Does the RAR indicate that the CSP is adequately staffed? (§4.3.1)	----

2	Does the RAR indicate a mature Change Management Capability? (§4.3.2)	----
3	Does the RAR show that CSP vendor dependencies and related agreements are adequately maintained? (§4.3.3)	----
4	Does the RAR indicate that the CSP has adequate Continuous Monitoring? (§4.3.4)	----
5	Does the RAR document the SSP maturity level? (§4.3.5)	----

Section G: Additional Comments

Information	
Report (RAR) Evaluation	
System Categorization:	(select)
Deployment Model:	(select)
Service Model:	(select)
Recommended by 3PAO?	
3PAO Name:	
ment for the Cloud Service Offering (CSO) named <CSO NAME>. This ur Third Party Assessment Organization (3PAO) <3PAO NAME.> This AMP Ready.	
Comments	
Comments	

Comments

--

Comments

l.3)	Comments

v.1.7

FEDRAMP RAR REVIEW PROCESS

DRAFT

Version 1.1
10/25/2017



FedRAMP



Revision History

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR



TABLE OF CONTENTS

1. GOALS:	1
2. RAR REVIEW PROCESS	1
2.1. 3PAO NOTIFY OF FUTURE SUBMISSION	1
2.2. 3PAO SUBMIT	1
2.3. CSP SUBMIT	1
2.4. SCHEDULE MEETING	1
2.5. MEETING AGENDA	2



I. GOALS:

- Collaborative RAR reviews in 4 hours
- Minimize back and forth discussions and updates between the FedRAMP PMO, the 3PAO, and the CSP
- Minimize incorrect reasoning surrounding misinterpretation of FedRAMP RAR requirements
- Maximize resource allocation (time, money, personnel) by real-time stakeholder collaboration

2. RAR REVIEW PROCESS

2.1. 3PAO NOTIFY OF FUTURE SUBMISSION

- 3PAO notifies PMO via info@fedramp when RAR will be submitted (Note: CSP submits RAR Evaluation Checklist in parallel with 3PAO RAR submission)
- Notification via info@fedramp must be at least a two-week timeframe

2.2. 3PAO SUBMIT

- 3PAO submits Moderate RARs via OMB MAX
- 3PAO must collaborate with the FedRAMP MAX Administrator for High RAR submissions

2.3. CSP SUBMIT

- CSP notifies PMO via info@fedramp when the RAR Evaluation will be submitted
- CSP RAR Evaluation must accompany the 3PAO RAR submission
- CSP submits RAR Evaluation using the FedRAMP CSP RAR Evaluation Checklist
- By signing the RAR Evaluation, the CSP is attesting that the CSP is aware that the 3PAO RAR submission is ready for FedRAMP analysis and review

2.4. SCHEDULE MEETING

- Preference is for all meetings to be in person
- Once a 3PAO and CSP submit the RAR and RAR Evaluation Checklist, the PMO sends suggested dates/times for the RAR collaboration meeting
 - **Attendees:** Must minimally include the CSP technical lead/ISSO, and the 3PAO assessment lead
 - The CSP and the 3PAO can invite as many people as required to ensure that all questions posed by the FedRAMP PMO concerning the Cloud Service Offering can be answered
 - 3PAO attendees must include a person who takes detailed notes that will be provided to all parties afterwards for confirmation of actions and next steps
 - In person attendance at GSA Building, 1800 F Street NW, Washington DC, is encouraged. Exceptions to in-person attendance must be coordinated with FedRAMP PMO within 5 days of proposed collaboration meeting time. If the CSP and/or 3PAO are not “local”, exception may be granted and video chat through WebEx or Google Hangouts is required



- **Dates / Time:** Meetings are held on Tuesday and Thursday morning or afternoon
- **Selection of Time:** Vendors can select the first available time that works for them on a first come, first served basis

2.5. MEETING AGENDA

- Time: 4 hours (minimal)
- Section Review Timeframe (estimated):
 - 1 hour for Sections 1-3
 - 3 hours for Section 4
- Review Schedule
 - PMO, CSP, and 3PAO read RAR together in real time
 - Notes are taken by all parties as they read documentation, and all questions must be asked in real time
 - RAR updates must be made in real time by the 3PAO as answers to questions are provided
 - Items that cannot be fixed immediately (e.g. network and data flow diagrams) must be discussed and diagrammed via whiteboard and/or paper until total stakeholder concurrence and acceptance is reached. The whiteboard and/or paper representation must then be incorporated precisely or better into the RAR by the 3PAO post meeting, as agreed by all stakeholders. Once the RAR has been read through in its entirety, the stakeholder team must read the RAR a second time to ensure RAR consistency and clear understanding.
 - After this exercise, there must be concise next steps and/or action items, to include a finalized RAR with all comments adjudicated. The next steps must be read out by the 3PAO note-taker and agreed to by all parties before the meeting adjourns
 - If the post-meeting outcome requires RAR resubmission:
 - The 3PAO updates the RAR with CSP feedback
 - 3PAO notifies info@fedramp that RAR has been re-submitted and is ready for PMO review
 - PMO re-reviews RAR
 - PMO notifies 3PAO/CSP of RAR re-review results
 - **Re-reviews that Pass:** RAR Evaluation report is posted to OMB MAX and the Marketplace is updated
 - **Re-reviews that Fail:** PMO requests a de-brief meeting with 3PAO, CSP, and PMO to discuss 3PAO's corrective action plan to submit a RAR that meets FedRAMP Ready standards



info fedramp <info@gsa.gov>

FedRAMP Connect Result

1 message

info fedramp <info@fedramp.gov>

Fri, Jan 22, 2021 at 4:03 PM

Bcc: (b) (6) @cisco.com, (b) (6) @cisco.com, (b) (6) @continuumgrc.com, (b) (6) @continuumgrc.com,
(b) (6) @ironnet.com, (b) (6) @ironnet.com, (b) (6) @mongodb.com, (b) (6) @mongodb.com,
(b) (6) @opusinteractive.com, (b) (6) @opusinteractive.com, (b) (6) @projecthosts.com, (b) (6) @projecthosts.com,
(b) (6) @axway.com, (b) (6) @axway.com, (b) (6) @yello.co, (b) (6) @yello.co

Dear CSP,

We regret to inform you that your Cloud Service Offering (CSO) has not been prioritized to pursue a JAB Authorization during our last round of FedRAMP Connect. Please let us know if you would like to have a follow up call to provide you feedback on your Business Case. Additionally, we would be happy to discuss the best authorization strategy for your CSO and ideas about opportunities for collaboration with agency customers. If you'd like to schedule a call, please e-mail info@fedramp.gov.

We look forward to continuing to work with you to achieve a FedRAMP Authorization.

Best,
FedRAMP PMO



[Contact Us](#) | [Manage Subscriptions](#) | [Unsubscribe All](#) | [Help](#)



info fedramp <info@gsa.gov>

IronNet Cybersecurity Inc. - IronCloud - 90-day FedRAMP Ready Extension

1 message

Ryan Hoelsing - QQC <ryan.hoelsing@gsa.gov>

Wed, May 19, 2021 at 9:51 AM

To: (b) (6) @ironnetcybersecurity.com

Cc: (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>,

(b) (6) <(b) (6) @ironnetcybersecurity.com>, info fedramp <info@fedramp.gov>, (b) (6)

<(b) (6) @gsa.gov>, (b) (6) - QQC-C <(b) (6) @gsa.gov>, (b) (6) - QQC-C

<(b) (6) @gsa.gov>, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C

(b) (6) @gsa.gov>, William Hamilton <william.hamilton@gsa.gov>

Hello (b) (6) and Team,

Currently, the PMO's guidance surrounding the *FedRAMP Ready* designation is that it is valid for one year from the date in which *FedRAMP Ready* was achieved. This is due to the fact that a RAR is a snapshot in time that provides agencies a sense of a service offering's capability of achieving a FedRAMP authorization.

However, given the current environment, a **90-day extension will be granted** from the date of IronNet Cybersecurity Inc. - IronCloud's original FedRAMP Ready expiration date of 7/29/2021.

Your new FedRAMP Ready expiration date is 10/29/2021. In order to remain on the FedRAMP Marketplace as "FedRAMP Ready", an updated FedRAMP Readiness Assessment **must be approved** by the FedRAMP PMO by this date. Please ensure you submit your updated RAR at least a month in advance to allow for adequate PMO review time. IronNet may also maintain a Marketplace listing by transitioning to "In Process" with a federal agency.

Please feel free to reach out to ryan.hoelsing@gsa.gov if you'd like to discuss your agency partnership strategy. Additionally, please let us know if you have any questions/concerns.

Best,
FedRAMP PMO

--

Ryan D. Hoelsing
FedRAMP - Customer Success Manager | COR III
Technology Transformation Service
GSA | TTS | 18F | FedRAMP
202 577 1938 - ryan.hoelsing@gsa.gov

"The mind is like a car battery - it recharges by running."
-Bill Watterson



info fedramp <info@gsa.gov>

Re: IronNet Cybersecurity Inc. - IronCloud - 90-day FedRAMP Ready Extension

1 message

Ryan Hoelsing - QQC <ryan.hoelsing@gsa.gov>

Fri, Oct 29, 2021 at 7:05 AM

To: (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6)@ironnetcybersecurity.com, (b) (6)@castus.tv, (b) (6)@castus.tv

Cc: (b) (6)@ironnetcybersecurity.com, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, info fedramp <info@fedramp.gov>, (b) (6) <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, William Hamilton <william.hamilton@gsa.gov>

Hello IronNet Cybersecurity Inc.,

I am following up on the above email. **IronNet Cybersecurity Inc. - Iron Cloud** has met the 90 day extension previously granted and the FedRAMP PMO has not approved a new RAR. In accordance with our guidance provided [FedRAMP Marketplace Designations for CSPs](#) **IronNet Cybersecurity Inc. - Iron Cloud** will be removed as *FedRAMP Ready* from the FedRAMP Marketplace by EOD today. **No additional extension will be granted.**

The FedRAMP PMO is responsible for maintaining the integrity of the Marketplace and a RAR is a snapshot in time that provides agencies a sense of a service offering's capability of achieving a FedRAMP Authorization. For this reason, RARs have a life cycle of one calendar year from the date of the *Ready* designation.

FedRAMP is committed to supporting **IronNet Cybersecurity Inc. - IronCloud** in your authorization efforts. **IronNet Cybersecurity Inc. - IronCloud** can be relisted on the Marketplace once the FedRAMP PMO has reviewed and approved a new RAR. We are also happy to jump on a call to discuss your authorization efforts to see if there is anything we can do to help in navigating the process.

Please let us know of questions and concerns.

Thank you,
Ryan Hoelsing

On Wed, May 19, 2021 at 9:51 AM Ryan Hoelsing - QQC <ryan.hoelsing@gsa.gov> wrote:

Hello (b) (6) and Team,

Currently, the PMO's guidance surrounding the *FedRAMP Ready* designation is that it is valid for one year from the date in which *FedRAMP Ready* was achieved. This is due to the fact that a RAR is a snapshot in time that provides agencies a sense of a service offering's capability of achieving a FedRAMP authorization.

However, given the current environment, a **90-day extension will be granted** from the date of IronNet Cybersecurity Inc. - IronCloud's original FedRAMP Ready expiration date of 7/29/2021.

Your new FedRAMP Ready expiration date is 10/29/2021. In order to remain on the FedRAMP Marketplace as "FedRAMP Ready", an updated FedRAMP Readiness Assessment **must be approved** by the FedRAMP PMO by this date. Please ensure you submit your updated RAR at least a month in advance to allow for adequate PMO review time. IronNet may also maintain a Marketplace listing by transitioning to "In Process" with a federal agency.

Please feel free to reach out to ryan.hoelsing@gsa.gov if you'd like to discuss your agency partnership strategy. Additionally, please let us know if you have any questions/concerns.

Best,
FedRAMP PMO

--

Ryan D. Hoelsing
FedRAMP - Customer Success Manager | COR III
Technology Transformation Service
[GSA](#) | [TTS](#) | [18F](#) | [FedRAMP](#)
202 577 1938 - ryan.hoelsing@gsa.gov

"The mind is like a car battery - it recharges by running."
-Bill Watterson

--

Ryan D. Hoelsing
FedRAMP - Customer Success Manager | COR III
Technology Transformation Service
[GSA](#) | [TTS](#) | [18F](#) | [FedRAMP](#)
202 577 1938 - ryan.hoelsing@gsa.gov

"The mind is like a car battery - it recharges by running."
-Bill Watterson



info fedramp <info@gsa.gov>

IronNet FedRAMP Connect Business Case

1 message

(b) (6) (b) (6) @ironnetcybersecurity.com>

Fri, Jun 10, 2022 at 3:22 PM

To: FedRAMP <info@fedramp.gov>

Cc: (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>

Taylor,

Please find enclosed the IronNet business case for this FedRAMP Connect cycle.

1. The JAB Prioritization Information Form
2. The Proof of Demand Worksheet


We appreciate your consideration, and look forward to hearing from you soon.


--
(b) (6)
IronNet Cybersecurity Inc.
Phone: (b) (6)
(b) (6) @ironnetcybersecurity.com
pmo@ironnetcybersecurity.com

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

2 attachments

 **IronNet Collective Defense Platform Demand Worksheet (10 June 2022).xlsx**
46K

 **IronNet_JAB_Prioritization_Business_Case_Form (10 June 2022).pdf**
1858K



FEDRAMP BUSINESS CASE

FOR JAB PRIORITIZATION

IronNet Cybersecurity

November 6, 2020

I. Cloud Service Provider (CSP) And Cloud Service Offering (CSO) Information

1.1 CSP Name: **IronNet Cybersecurity, Inc.**

1.2 System Name: **IronNet Cloud**

1.3 CSP Website: <https://www.ironnet.com/>

1.4 Two Points of Contact

(Name, Email, and Phone Number):

(b) (6),
(b) (6)@ironnet.com,
(b) (6),
(b) (6)@ironnet.com, (b) (6)

1.5 Cloud service Model:

- ☒ SaaS
☐ IaaS
☐ PaaS

1.6 Deployment Model:

- ☒ Public Cloud
☐ Government Only Cloud
☐ Fed Government Only Cloud
☐ DoD Cloud

1.7 FIPS 199 Impact Level:

- ☐ High
☒ Moderate
☐ Low

1.8 a Do you own your entire infrastructure? ☒ No ☐ Yes

1.8 b If no, what is the name of the JAB Authorized infrastructure you are using?

(If you are using an Agency Authorized infrastructure, you are not eligible for a JAB P-ATO.)

AWS GovCloud

1.9 Is the CSO FedRAMP Ready? ☐ No ☒ Yes

The CSO currently has the following certifications:

2. IronNet is ISO/IEC 27001:2013 Certified and SRI Quality System is our Registrar through ANAB (Certifying body), our certificate #020111 is valid through November 12, 2020. We have successfully completed our 3-year unconditional renewal, pending final report due mid-November.

Besides the SOC2 Types I & II and the ISO/IEC 27001 listed above for the past three years, the CSP is also GDPR-Compliant since 2018. This consistent and independantly audited history of meeting Information Security Management Systems standards since 2017 demonstrates a proven track record of mature organizational processes.

The CSO aligns with National Cybersecurity Strategy, Sep 2018, Pillar I by providing network detection and response and collective defense capabilities to secure Federal Networks and Information, secure Critical Infrastructure, and combat Cybercrime and Improve Incident Reporting. IronNet in 2018 received two separate acceptances/approvals for the DHS Continuous Diagnostics & Monitoring Approved Products List (CDM APL) for IronDefense (IRO-0002-20180103) and IronDome (IRO-0004-20180405).

2. Brief Service Description:

In the space below, provide a brief description of your service and the value it would bring to the Federal Government. Questions this write-up should address include:

- 1) How does an agency use and experience you offering?
- 2) How is your CSO broadly applicable across the Federal Government?
- 3) Does your CSO provide a new and innovative service?
- 4) Why should the JAB authorize your service over similar offerings?

IronNet Cloud with FedRAMP (IronDefense / IronDome) provides a cloud-based network behavioral analytics platform for customers to detect network-based malicious traffic on all five stages of the cyber security kill chain: Reconnaissance, Access, C2, Action, and 'other'. (Note: The use of "other" in this context is used as a catch-all for items not classified in the cyber security kill chain. The other classification, allows the algorithms to process the kill chain for items unknown in class, or the other classification.)

IronDefense processes customer and agency metadata, network traffic for threat behavioral analytics, and integrated hunt algorithms to detect malicious threat traffic. IronDefense and IronDome combines capabilities to provide the industry's first collective defense solution that links industry peers, third-party suppliers, and other stakeholders into a joint defense infrastructure.

With the rise of cyber attacks during the COVID-19 pandemic and the resulting economic crisis, we need to better understand threats and work together, collectively, in order to stop them. Our federal critical infrastructure and the wealth of our country are at risk. State by state, and as a nation, identifying unknown threats and collaborating to defend against them in real-time are critical to our success. In other words, cybersecurity is national security and is applicable across our entire Federal Government. Consider our current situation:

- Nation-state adversaries and other major threat actors have their eye on American critical infrastructure and other key systems across the public and private sectors. In 2018, for example, the U.S. publicly accused Russia of conducting a two-year long coordinated campaign of cyber intrusions into the U.S. grid.

- Adversaries are seeking to take advantage of new vulnerabilities in the midst of the current pandemic.

Cybersecurity agencies from the U.K., Canada, and the U.S. recently attributed a campaign targeting pharmaceutical companies and academic institutions involved in COVID-19 vaccine development to APT29, a group widely believed to be operating on behalf of Russian intelligence services.

- New levels of remote working and learning are increasing vulnerabilities. The education sector has reported the highest percentage (61%) of enterprise malware attacks of all industries in the last 30 days, according to Microsoft Security Intelligence.

IronDefense / IronDome is the path to Collective Defense and how Federal Agencies can gain the knowledge needed and the ability to collaborate at the speed of attack.

What makes Collective Defense such a powerful tool is the cyber threat sharing platform that allows participating organizations to become aware of and thwart cyber attacks targeting similar organizations. By sharing cyber anomalies in real time across a community of peers and within situational context, companies can identify attackers earlier in the attack cycle (that is, the cyber kill chain) when many of their methods fall below the threshold of detection. In other words, behavioral analytics can detect "unknown unknowns," making this new approach to cybersecurity a stronger defense approach than signature-based analytics often used in Network Traffic Analysis (NTA) solutions. Collective Defense sharing complements Information Security and Analysis (ISAC) groups and Threat Intelligence Platforms (TIPs).

1.10 If applicable, provide details of certifications (SOC2, ISO27001, PCI, etc.) that demonstrate that your CSO has been assessed for security in other compliance regimes proving a track record of security compliance.

The CSO currently has the following certifications:

1. IronNet is SOC2/Type I and Type II through KirkpatrickPrice LLC as our Auditor. Initially audited in June 2017 under Type I criteria, confirming we have a suitable Design of Controls to meet the criteria for the Security, Availability, Confidentiality, Processing, and Integrity principles of the SOC2 standard. In August 2018 we obtained our Type II attestation that demonstrated operational effectiveness of our design controls and continue annual audits.
2. IronNet is ISO/IEC 27001:2013 Certified and SRI Quality System is our Registrar through ANAB (Certifying body), our certificate #020810 is valid through November 2, 2023. We have successfully completed our 3-year unconditional renewal, and continue annual surveillance audits.

1.11 If applicable, provide details around proven maturity (CMMI Level 3+, ISO Organizational Certifications, etc.) that demonstrate a proven track record of mature organizational processes that increase the likelihood that you will be able to maintain an acceptable risk posture.

Besides the SOC2 Types I & II and the ISO/IEC 27001 listed above for the past three years, the CSP is also GDPR-Compliant since 2018. This consistent and independantly audited history of meeting Information Security Management Systems standards since 2017 demonstrates a proven track record of mature organizational processes.

1.12 If applicable, provide details on how your CSO aligns with administrative priorities for cross-agency services. Examples of OMB Policy, Priorities, and Shared Services could include (but are not limited to): Alignment with National strategy and policies; CSP provides a new solution to existing Federal requirements (such as CDM or HSPD-12); CSP provides a solution for existing Federal mandates where there are large areas of agency deficiencies.

The CSO aligns with National Cybersecurity Strategy, Sep 2018, Pillar I by providing network detection and response and collective defense capabilities to secure Federal Networks and Information, secure Critical Infrastructure, and combat Cybercrime and Improve Incident Reporting. IronNet in 2018 received acceptances/approvals for the DHS Continuous Diagnostics & Monitoring Approved Products List (CDM APL) for IronDefense (SKUs: IDT-0100-12, IDT-0500-12 and IDT-1000-12) and was renewed in February, 2021.



2. Brief Service Description:

In the space below, provide a brief description of your service and the value it would bring to the Federal Government. Questions this write-up should address include:

- 1) How does an agency use and experience you offering?
- 2) How is your CSO broadly applicable across the Federal Government?
- 3) Does your CSO provide a new and innovative service?
- 4) Why should the JAB authorize your service over similar offerings?

IronNet's Collective Defense Platform provides a cloud-based network analytics and correlations platform for customers to detect network-based malicious traffic on all five stages of the cyber security kill chain: Reconnaissance, Access, C2, Action, and 'other'. (Note: The use of "other" in this context is used as a catch-all for items not classified in the cyber security kill chain. The other classification, allows the algorithms to process the kill chain for items unknown in class, or the other classification).

The Platform processes customer and agency metadata, log data, network traffic, data from current cyber security stack(s) including cloud service providers. It leverages advanced network detection and response capabilities (NDR) to detect and prioritize anomalous activity inside individual networks along with integrated workflows for alert prioritization. The Platform analyzes threat detections across networks to identify broad based attack patterns. The Platform generates intelligence for community members in real time that can be shared with participating members for early insight into potential incoming attacks.

With CoVID, adversaries have refined their tradecraft to become more sophisticated. A series of high profile attacks have rocked many organizations and, on their own, represent watershed moments in the cybersecurity threat landscape. During 2021, organizations have scrambled to protect supply chains, critical infrastructure and interconnected systems and were faced with incredibly sophisticated attacks like Sunburst attack, Colonial Pipeline attack, along with exploitation of zero-day vulnerabilities in Microsoft leaving many reeling. State by state, and as a nation, identifying unknown threats and collaborating to defend against them in real-time are critical to our success. In other words, cybersecurity is national security and is applicable across our entire Federal Government. Consider our current situation from 2021:

- Chinese actors focussed significant attention on series of vulnerabilities in Microsoft Exchange (ProxyLogon and ProxyShell) to launch intrusions
- Log4j zero-day exploit attributed to a Nationstate identified and reported in late Nov 2021 resulting in many state actors / APT actors integrating the exploits into their tool chain.
- Critical infrastructure attacks such as the ransomware targeted at Colonial pipeline causing disruption in the oil distribution and increasing pain at the pump for US consumers

IronNet's solution is the first step in the path to Collective Defense and how Federal Agencies can gain the knowledge needed and the ability to collaborate at the speed of attack.

Collective Defense can be a powerful capability when the cyber threat exchange platform allows participating organizations to become aware of and thwart cyber attacks targeting similar organizations. Through real time threat exchange of cyber anomalies across a community of peers and within situational context, organizations will be able to identify attackers earlier in the attack cycle (that is, the cyber kill chain) when many of their methods fall below the threshold of detection. In other words, analytics and correlations will detect "unknown unknowns," making this new approach to cybersecurity a stronger defense approach than signature-based analytics often used in Network Traffic Analysis (NTA) solutions. Collective Defense threat exchange complements Information Security and Analysis (ISAC) groups.



info fedramp <info@gsa.gov>

Request: Call with FedRAMP PMO re: FedRAMP Connect

1 message

info fedramp <info@fedramp.gov>

Fri, Jul 29, 2022 at 10:09 AM

To: (b) (6) @ironnet.com, (b) (6) @ironnet.com

Cc: (b) (6) - QQC-C <(b) (6) @gsa.gov>, (b) (6) - QQC-C <(b) (6) @gsa.gov>, (b) (6) - QQC-C <(b) (6) @gsa.gov>

(b) (6)

The FedRAMP PMO would like to thank you for participating in FedRAMP Connect and submitting Iron Net's business case for JAB prioritization. In order to make a final decision on which CSPs will be prioritized to work with the JAB, we'd like to meet with you to hear more about your system architecture. ***Please provide Megan Gallo (cc'd on this email) with 2-3 time slots that work for you and your team to have a call with the PMO before August 10th and we will send a calendar invite with a conference line.***

During this meeting we'd like you to provide a presentation on the following information:

- Describe your authorization boundary.
- Describe all external services and corporate services that you use.
 - Please review the [FedRAMP Boundary Guidance document](#) available on FedRAMP.gov
- Describe any system connections/interconnections the JAB should be aware of.
- Describe your compliance with FIPS 140-2 validated encryption and provide the cert numbers for your FIPS compliance.
- Describe your solution for meeting the DNSSEC requirements.
- Describe your multi-factor authentication implementation.
 - Please note that compliance with FIPS 140-2 is required for MFA devices.
- Detailed timeline for becoming FedRAMP Ready per JAB standards, including any system/architecture changes required
 - Please note that unlike an Agency Authorization or Agency FedRAMP Ready designation, the JAB does not accept risk and precludes the use of external services that contain customer data.

Please provide this presentation at least two business days prior to your call so we can prepare any questions we may have. The people from your organization on the call should be able to discuss these topics (this is not a sales call). If you have any questions about the information being requested, please feel free to reach out.

We look forward to speaking with you soon.

All the best,
FedRAMP PMO

**FedRAMP PMO**

FedRAMP | TTS | GSA

Contact Us | Manage Subscriptions





(b) (6) - QQC-C <(b) (6)@gsa.gov>

IronNet Slides for 10 Aug

2 messages

Fernando Maymi <(b) (6)@ironnet.com>

Mon, Aug 8, 2022 at 9:46 PM

To: (b) (6)@gsa.gov

Cc: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6)@ironnetcybersecurity.com>, (b) (6)@ironnetcybersecurity.com>, (b) (6)@ironnetcybersecurity.com>



(b) (6)@ironnet.com is using Virtru to send and receive encrypted email.

Unlock Message

UNENCRYPTED INTRODUCTION

To view my encrypted message, you'll need to verify your identity. Please contact me if you have any questions.

[Having trouble viewing this message?](#)

© Copyright 2022 Virtru Corporation | [Terms of Service](#) | [Privacy Policy](#) | [About Virtru](#) | [Support](#)

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

(b) (6) - QQC-C <(b) (6)@gsa.gov> Tue, Aug 9, 2022 at 4:33 PM
To: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

[Quoted text hidden]

--



U.S. General Services Administration

(b) (6)
Technology Transformation Services
FedRAMP | Max.gov Transition
(b) (6) @gsa.gov | (b) (6)



(b) (6) - QQC-C <(b) (6)@gsa.gov>

IronNet FedRAMP Application

1 message

(b) (6) <(b) (6)@ironnet.com>

Wed, Aug 10, 2022 at 12:52 PM

To: (b) (6)@gsa.gov

Cc: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>

(b) (6)

Thanks, again, to you and your team for your time and inputs today. I just wanted to update you on our expected timeline. Upon further reflection, we would like to commit to sending you the complete application (SSP, SAP, SAR, and POA&M) by May 2023 (assuming, of course, that we are selected by the JAB for prioritization). This should give you three months before final certification, which we expect would be accomplished by August as we showed on the slide.

Please let me know if you have any questions. Thanks!

(b) (6)

(b) (6)

Chief Information Security Officer, IronNet

m: +(b) (6)

(b) (6)@ironnetcybersecurity.com

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.



(b) (6) - QQC-C <(b) (6)@gsa.gov>

Congratulations on Being Prioritized for a FedRAMP JAB Authorization

6 messages

info fedramp <info@fedramp.gov>

Mon, Oct 24, 2022 at 9:59 AM

To: (b) (6)@ironnet.com, (b) (6)@ironnet.com

Cc: Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

Dear (b) (6),

Based on IronNet's high level of demand and the quality of your business case, your CSO has been prioritized to go through the JAB authorization process. This prioritization decision was made by the JAB TRs, approved by GSA's Office of General Counsel and JAB CIOs, and shared with the CIO Council.

To jump-start the next phase of your work with FedRAMP, the PMO would like to have a one-on-one call with you and your team about next steps. **Please e-mail claire.bukovac@gsa.gov and megan.gallo@gsa.gov with 4-5 time slots your team is available to meet** and we'll send a calendar invite with a conference line.

During this meeting please be prepared to discuss the following:

- **JAB FedRAMP Ready and Security Package Submission Timeline**
 - Please be prepared to provide clear milestones and dates associated with becoming FedRAMP Ready to JAB standards and submitting a full security package (SSP, SAP, SAR, POA&M, first month of ConMon).
- **Next Steps and Meeting Cadence with the PMO**
 - The FedRAMP PMO will walk you through what to expect now that your offering has been prioritized for a JAB P-ATO. The PMO will have regular calls with you and your team as you work toward kicking off with the JAB to ensure continued progress toward milestones. Come prepared to discuss scheduling availability for your organization to attend these regular meetings.
- **Questions Regarding Relevant Guidance**
 - Prior to the call, please be familiar with the following guidance documents and prepare any questions you have on this information.
 - [CSP's JAB Authorization Roles and Responsibilities](#)
 - [FedRAMP Authorization Boundary Guidance](#)
 - [Timeliness and Accuracy of Testing Requirements](#)
- **Press Release Guidance**
 - Given the sensitive elements involved in this process, we ask that you don't publicly release information until the PMO has announced this prioritization decision. During the call we will provide guidance on what you can share publicly after the PMO's announcement about your CSO being prioritized to work with the JAB. All planned communication must be provided to the FedRAMP PMO prior to publishing.

The JAB looks forward to working with you!

Best,
FedRAMP PMO

**FedRAMP PMO**

FedRAMP | TTS | GSA

[Contact Us](#) | [Manage Subscriptions](#)

(b) (6) <(b) (6)@ironnetcybersecurity.com> Mon, Oct 24, 2022 at 1:10 PM
To: (b) (6) - QQC-C <(b) (6)@gsa.gov>
Cc: (b) (6)@ironnet.com, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C
(b) (6)@gsa.gov, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6)
<(b) (6)@ironnetcybersecurity.com>

Claire and team,
Great news to kick off the week. We will be back with date/times to schedule a VTC.

Thank you,

(b) (6)

(b) (6)

VP Americas Public Sector Sales

Mobile: (b) (6)

[LinkedIn](#) | [Twitter](#) | [Gartner Peer Insights](#) | [IronRadarsm](#)



[Quoted text hidden]

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

(b) (6) <(b) (6)@ironnetcybersecurity.com> Wed, Oct 26, 2022 at 9:34 AM
To: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6)
<(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnet.com>
Cc: (b) (6)@ironnet.com, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C
<(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

(b) (6)

Thank you for the exciting news. We have the following dates/times available next week:

- Monday - 1-3
- Wednesday - 1-4

- Thursday - 2-4

Thank you,

(b) (6)

(b) (6)

VP Americas Public Sector Sales

Mobile: (b) (6)

LinkedIn | Twitter | Gartner Peer Insights | **IronRadarsM**



[Quoted text hidden]

[Quoted text hidden]

(b) (6) <(b) (6)@ironnetcybersecurity.com>

Wed, Nov 2, 2022 at 1:21 PM

To: (b) (6) - QQC-C <(b) (6)@gsa.gov>

Cc: (b) (6)@ironnet.com, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C

<(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6)

<(b) (6)@ironnetcybersecurity.com>

(b) (6)

Are you available in the afternoon next Monday, Tuesday, Wednesday?

(b) (6)

(b) (6)

VP Americas Public Sector Sales

Mobile: (b) (6)

LinkedIn | Twitter | Gartner Peer Insights | **IronRadarsM**



[Quoted text hidden]

[Quoted text hidden]

(b) (6) - QQC-C <(b) (6)@gsa.gov>

Wed, Nov 2, 2022 at 3:48 PM

To: (b) (6) <(b) (6)@ironnetcybersecurity.com>

Cc: (b) (6)@ironnet.com, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C

<(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6)

<(b) (6)@ironnetcybersecurity.com>

Hi (b) (6)

Thank you for following up and apologies for the delay - I was out sick last Wednesday and this must have fallen through the cracks.

Would one of the following times work for you? I'll send a calendar invite for whichever time works best.

- Monday, November 7th at 1:00pm ET
- Tuesday, November 8th at 12:00pm ET
- Tuesday, November 8th at 2:30pm ET
- Wednesday, November 9th at 2:00pm ET

Thanks!

(b) (6)

[Quoted text hidden]



U.S. General Services Administration

(b) (6)

Technology Transformation Services
FedRAMP | Max.gov Transition

(b) (6) @gsa.gov | (b) (6)

(b) (6) <(b) (6) @ironnetcybersecurity.com>

Wed, Nov 2, 2022 at 3:55 PM

To: (b) (6) - QQC-C <(b) (6) @gsa.gov>, (b) (6) <(b) (6) @ironnetcybersecurity.com>

Cc: (b) (6) @ironnet.com, Brian Conrad - QQC <brian.conrad@gsa.gov>, (b) (6) - QQC-C

<(b) (6) @gsa.gov>, (b) (6) - QQC-C <(b) (6) @gsa.gov>, (b) (6)

<(b) (6) @ironnetcybersecurity.com>

Wednesday works. Please include Alsa and Raj from IronNet.

(b) (6)

(b) (6)

VP Americas Public Sector Sales

Mobile: (b) (6)

LinkedIn | Twitter | Gartner Peer Insights | **IronRadarsM**



[Quoted text hidden]

[Quoted text hidden]



(b) (6) - QQC-C <(b) (6)@gsa.gov>

JAB Prioritization for IronNet

1 message

(b) (6) <(b) (6)@ironnetcybersecurity.com> Wed, Nov 9, 2022 at 2:42 PM
To: (b) (6)@gsa.gov, (b) (6)@gsa.gov, (b) (6)@gsa.gov
Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnet.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>

Thank you for going over the guidance and answering our questions about the JAB Authorization process! We look forward to working with you and will keep in touch as we progress. I've attached our current timeline and will be sure to provide any updates as they are needed.


Sincerely,

--

(b) (6)
Director, GRC
IronNet Cybersecurity Inc.
Phone: (b) (6)
(b) (6)@ironnetcybersecurity.com

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

 **JAB P-ATO Timeline ao 9 Nov 22.pptx**
991K

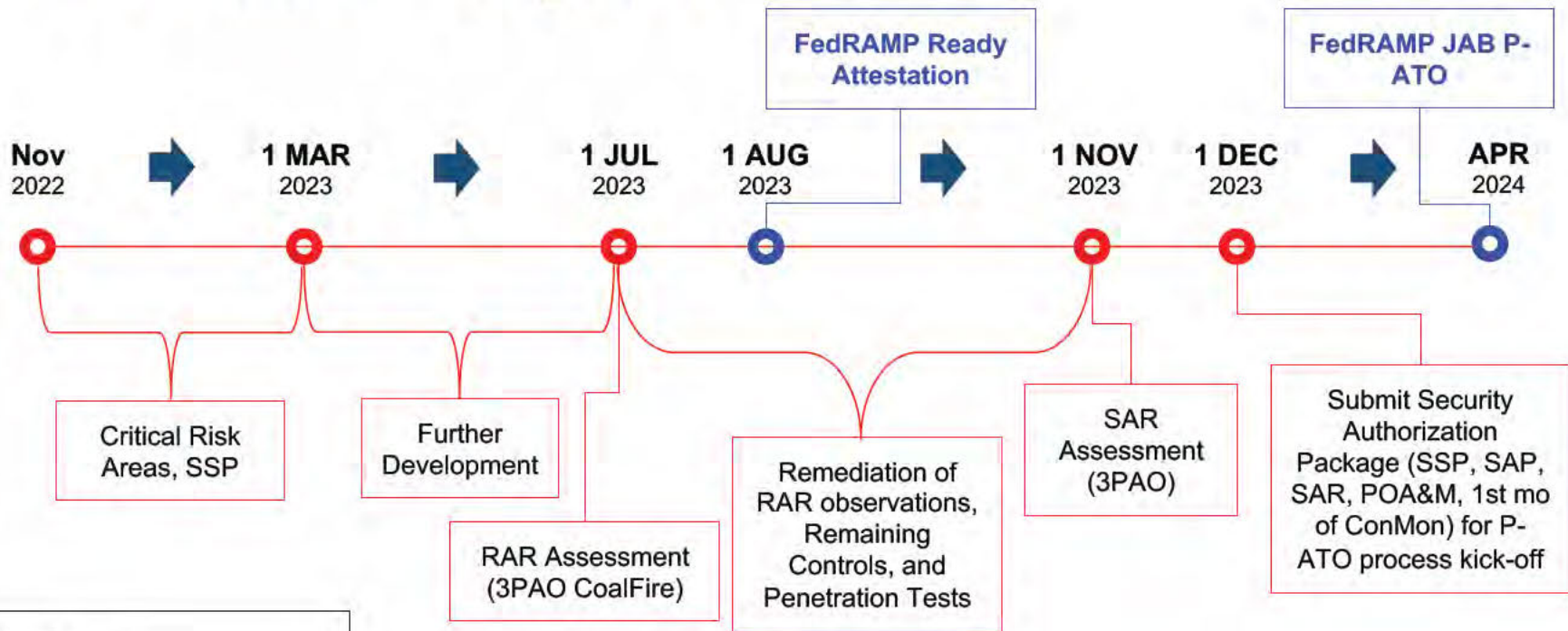


IronNet Collective Defense

Presentation to the FedRAMP PMO

9 November 2022

FedRAMP Targeted Timeline



Acronym Key:

- System Security Plan (SSP)
- Readiness Assessment Report (RAR)
- 3rd Party Assessment Office (3PAO)
- Security Assessment Report (SAR)
- Joint Advisory Board Prog Mgmt Office (JAB PMO)
- Security Assessment Plan (SAP)
- Program of Action & Milestones (POA&M)
- Continuous Monitoring (ConMon)
- Provisional Authority to Operate (P-ATO)



(b) (6) - QQC-C <(b) (6)@gsa.gov>

IronNet Release on JAB Selection

6 messages

(b) (6) <(b) (6)@ironnet.com>

Mon, Nov 28, 2022 at 11:05 AM

To: (b) (6)@gsa.gov

Cc: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>

(b) (6)

I hope you had a nice Thanksgiving break. As you requested, attached is our proposed media release on our selection by the JAB. Would you please review it at your earliest convenience and let us know if we are good to go? We are hoping to release it this Wednesday or Thursday if you have no objections. Thanks for your time.

(b) (6)

(b) (6)

Chief Information Officer, IronNet

m: (b) (6)

(b) (6)@ironnetcybersecurity.com

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.



IronNet Prioritized by FedRAMP_Press Release vfinal2 for JAB approval.docx

18K

(b) (6) <(b) (6)@ironnetcybersecurity.com>

Tue, Nov 29, 2022 at 5:25 PM

To: (b) (6) <(b) (6)@ironnet.com>

Cc: (b) (6)@gsa.gov, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

Thank you (b) (6) -- I appreciate your sharing our draft.

It's a pleasure to meet you, (b) (6) and team. I hope this second draft meets with your approval. As (b) (6) mentioned, IronNet hopes to issue it pre-market on Thursday.

Thank you in advance for confirming.

Best,

(b) (6)

(b) (6)

IronNet, Inc. (NYSE: IRNT)

Direct: (b) (6)



[Quoted text hidden]

[Quoted text hidden]

(b) (6) <(b) (6)@ironnet.com>

Wed, Nov 30, 2022 at 4:00 PM

To: (b) (6)@gsa.gov

Cc: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>

(b) (6)

Just floating this to the top of your inbox since I'm pretty sure you're swamped. Any chance we can get the greenlight today or early tomorrow? Thanks!

(b) (6)

(b) (6)

Chief Information Officer, IronNet

m: (b) (6)

(b) (6)@ironnetcybersecurity.com

[Quoted text hidden]

[Quoted text hidden]

(b) (6) <(b) (6)@ironnetcybersecurity.com>

Wed, Nov 30, 2022 at 7:49 PM

To: (b) (6) <(b) (6)@ironnet.com>

Cc: (b) (6)@gsa.gov, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

Hi again (b) (6) -- can you kindly let us know if this is in your process or if you would require us to seek approval elsewhere? I noted that a few similar releases have been issued t in the last day by other cyber companies, our approval has actually been referenced by other parties in social media, but we'd like to be the one to report out. We respect your process and want to ensure we have your approval. We'd really appreciate an update.

Thank you very much!

(b) (6)

IronNet Communications

[Quoted text hidden]

[Quoted text hidden]

(b) (6) - QQC-C <(b) (6)@gsa.gov>

Fri, Dec 2, 2022 at 10:22 AM

To: (b) (6) <(b) (6)@ironnetcybersecurity.com>

Cc: (b) (6) <(b) (6)@ironnet.com>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

Hi (b) (6)

Apologies for the delay. This is approved!

Thanks!

(b) (6)

[Quoted text hidden]

--



U.S. General Services Administration

(b) (6)

Technology Transformation Services
FedRAMP | Max.gov Transition

(b) (6)@gsa.gov | (b) (6)

(b) (6) <(b) (6)@ironnetcybersecurity.com>

Fri, Dec 2, 2022 at 10:51 AM

To: (b) (6) - QQC-C <(b) (6)@gsa.gov>
Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnet.com>, (b) (6)
- QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>

Thank you (b) (6) Really appreciate your review and approval.

We will issue this Monday after market.

Best regards,

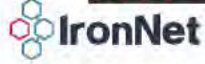
(b) (6)

[Quoted text hidden]

--

(b) (6)

VP of Investor Relations
IronNet, Inc. (NYSE: IRNT)
Direct: (b) (6)



[Quoted text hidden]

IronNet Prioritized by FedRAMP Joint Authorization Board to Pursue Provisional Authority to Operate

MCLEAN, Va. (DATE, 2022) – IronNet, Inc. (NYSE: IRNT), an innovative leader Transforming Cybersecurity Through Collective DefenseSM, announced today it has been prioritized by the United States Federal Risk and Authorization Management Program (FedRAMP) to pursue a Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB).

FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. As the primary governance and decision-making body for FedRAMP, the JAB is comprised of the Chief Information Officers from the Department of Homeland Security, General Services Administration, and Department of Defense.

“Prioritization to pursue a P-ATO is an important step towards expanding the deployment of the IronNet Collective Defense platform into more federal agencies. As cyber attacks become increasingly more sophisticated, any organization that is still attempting to defend its networks alone is accepting unnecessary risk,” said General (Ret.) Keith Alexander, CEO and Founder of IronNet. “Our unique Collective Defense platform includes advanced behavioral analytics and leverages a sophisticated expert system to reduce false positives in order to defend against global cyber attacks. We’re committed to the FedRAMP process to deliver this protection to government agencies at scale as we continue working together to strengthen our nation’s cyber defense.”

The goal of the FedRAMP program is to grow the use of secure cloud technologies in use by government agencies and enhance the framework by which the government secures and authorizes cloud technologies. IronNet is pursuing FedRAMP High certification to help protect the government’s most sensitive, unclassified data in cloud computing environments.

The IronNet Collective Defense platform, powered by AWS, identifies anomalous behaviors and delivers actionable attack intelligence to all the other participants in the IronNet community. The Collective Defense platform serves as an early warning system for all participating companies and organizations, strengthening network security through correlated alerts, automated triage, and extended hunt support.

About IronNet, Inc.

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Forward-Looking Statements

This press release includes “forward-looking statements” within the meaning of the “safe harbor” provisions of the United States Private Securities Litigation Reform Act of 1995, including, without limitation, statements regarding IronNet’s ability to provide visibility and detection of malicious behaviors and to help defend against increased cyber threats facing the globe and IronNet’s plans to pursue a P-ATO and FedRAMP High certification and expand the deployment of the IronNet Collective Defense platform into more federal agencies. When used in this press release, the words “estimates,” “projected,” “expects,” “anticipates,” “forecasts,” “plans,” “intends,” “believes,” “seeks,” “may,” “will,” “should,” “future,” “propose” and variations of these words or similar expressions (or the negative versions of such words or expressions) are intended to identify forward-looking statements. These forward-looking statements are not guarantees of future performance, conditions, or results, and involve a number of known and unknown risks, uncertainties, assumptions and other important factors, many of which are outside IronNet’s management’s control, that could cause actual results or outcomes to differ materially from those discussed in the forward-looking statements. Important factors, among others, that may affect actual results or outcomes include: IronNet’s inability to recognize the anticipated benefits of collaborations with IronNet’s partners and customers; IronNet’s ability to execute on its plans to develop and market new products and the timing of these development programs; the rate and degree of market acceptance of IronNet’s products; the success of other competing technologies that may become available; IronNet’s ability to identify and integrate acquisitions; the performance of IronNet’s products; potential litigation involving IronNet; and general economic and market conditions impacting demand for IronNet’s products. The foregoing list of factors is not exhaustive. You should carefully consider the foregoing factors and the other risks and uncertainties described under the heading “Risk Factors” in IronNet’s Annual Report on Form 10-K for the year ended January 31, 2022, filed with the Securities and Exchange Commission (the “SEC”) on May 2, 2022, IronNet’s most recent Quarterly Report on Form 10-Q for the quarter ended July 31, 2022, filed with the SEC on September 14, 2022, and other documents that IronNet files with the SEC from time to time. These filings identify and address other important risks and uncertainties that could cause actual events and results to differ

materially from those contained in the forward-looking statements. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and IronNet does not undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.

Contacts:

Investor Contact: IR@ironnet.com

Media Contact: Media@ironnet.com

IronNet - FedRAMP Connect System Information Call
August 10, 2022 10:00am

Resources:

- [Folder](#)
- Presentation- Separate in email
- Follow up E-mail: Thanks, again, to you and your team for your time and inputs today. I just wanted to update you on our expected timeline. Upon further reflection, we would like to commit to sending you the complete application (SSP, SAP, SAR, and POA&M) by May 2023 (assuming, of course, that we are selected by the JAB for prioritization). This should give you three months before final certification, which we expect would be accomplished by August as we showed on the slide.

Attendees

PMO:

- (b) (6)
- (b) (6)
- (b) (6)

Iron Net:

- (b) (6), CISO (Asshat)
- (b) (6), VP Platform Engineering
- (b) (6), VP Architecture and Innovation (really cool dude)
- (b) (6), IronNet Security Engineering Architect (TBD)
- (b) (6), IronNet Principal Systems Architect
- (b) (6), Technical Program Manager
- (b) (6), SOC Chief
- (b) (6) Product Security Engineer

Agenda:

- Describe your authorization boundary
 - Two ways to collect information from customers (on prem and collecting information from cloud environments)
 - Sam: External from boundary- these are actually leverage services. It is important to call them this so it doesn't confuse anyone later (will change slide to say FedRAMP high leverage services)
 - 8 services total (Cloud Trail, Cloud Watch, Cognito, DynamoDB, EKS, IAM, MSK, Kinesis)
 - Network configuration tools- all FedRAMP High compliant- 9 total (NAT, NLB, Opensearch, RDS, Amazon SNS, and SQS....)
- Describe all external services and corporate services that you use
 - Architecture

- First, we have 5 different X to give functionality. Second, we have an org dedicated to delivering platform services and just because the services are high, it doesn't mean that they are utilized that way. We have one team dedicated to bringing these to the platform and make sure all services integrated are high. Third,
- External Connections
 - SAML- This is the MFA (multi-factor)
 - Jump Host
 - Customer User Access- This is where the user/client gets on their laptop and wants to access our system
 - #4 and 5- Related where the information from our clients comes back into our network so we can analyze it
- Describe any system connections/interconnections the JAB should be aware of.
 - We know very well how our systems are organized and who is talking to who
 - We very well know our structure and integration
- Describe your compliance with FIPS 140-2 validated encryption and provide the cert numbers for your FIPS compliance.
 - We take this very seriously and know its important for FedRAMP high
 - We know that all of these services are FedRAMP high, and if we switch the right buttons on, we can validate that they are either encrypted at rest or encrypted in motion
- Describe your solution for meeting the DNSSEC requirements.
 - We are using route 53 and CKS (this also uses route 53)
 - Internal routing- Using Route 53 configurations
 - DNS external services- how do people reach us- We are looking for customers to provide a level of DNS services to find us
- Describe your multi-factor authentication implementation.
 - Please note that compliance with FIPS 140-2 is required for MFA devices.
- Detailed timeline for becoming FedRAMP Ready per JAB standards, including any system/architecture changes required
 - Based on our experience based on the readiness for the moderate level
 - We already have a 3PAO scheduled to come after Thanksgiving. This gives us 90 days to do the ConMon
 - We need to tighten up our documentation- we are about 60% there
 - We need to make sure our POA&M is correct too
 - We know that there is going to be some period of time during this timeline that we are going to need access to a CAC or PIV system
 - We expect there will be remediation time after we meet with the 3PAO that they ask us to address and expect the SAR to come back in May. We assume we will have to go back and forth with the 3PAO after the SAR submission as well
 - We expect this will be the same if we want to go through the JAB process too
 - Sam: You may have to parse the language on this when presenting to the JAB

- (b) (6) Yes, but we have time. It's ok if we are not within the 30/60/90 days. But, where did you hear that you had to have 90 days of ConMon before the readiness assessment?
 - (b) (6) That was part of Telos.
- February 2023- submitting the RAR
- July 2023- they will submit their full JAB submission package
- August 2023- Full authorization milestone goal

Notes:

- 40 entities within the DIB side, also have 80 entities outside that space
- Authorization Boundary
 - Two modalist to collect info from customers - on-premise and collecting info from cloud environment - those are the two entry points into our system
 - Customer interact with system: supporting two access token - dua and CAC token - required to connect in to system
 - Using cognito - federated ID provider for AWS - reaches out to SAML depending on the token being presented
 - Admin - login to VPN alto provider with hard token MFA enables, once auth is established, can log in to jump box - the jump box is where they iterate with everything in the boundary
 - From the jump box, able to interact with VPCs
 - Sam's Questions/feedback:
 - Duo integration - just passing SAML assurance? Not holding names? Correct
 - Two entry points - for this authorization those would need to be included in your boundary and tested
 - Can't be in a user environment and not tested
 - IronNet: absolutely consider those sensitive, may be not accurately represented in boundary diagram
 - Five layers to system - ETL layer, enrichment phase, correlations engine, web UI
 - Using cooper netties for distribution, load balancing and house and scale code
 - Question: All these AWS services are at high?
 - Yes, all are already FedRAMP high certified
 - Sam: these are leveraged services, not external services, they are considered part of your boundary - could confused people in the future
- External Services:
 - All the "external services" are leveraged services and they are FedRAMP High complaint

FedRAMP Business Case: Proof of Demand Worksheet

In order to accurately evaluate demand, the FedRAMP PMO has developed this excel worksheet for CSPs to complete.

Instructions:

- 1) Complete each relevant tab with the required information. We will not contact any of the references provided without your knowledge.
- 2) Do NOT PDF this excel. Save your completed excel worksheet as "[CSP's Name] Demand Worksheet [Submission Date]."
- 3) Submit your completed excel worksheet to info@fedramp.gov WITH your JAB Prioritization Information Form.

complete in order to show proof of 1)

nowledge and consent. If you have questions

Instructions: List all current Federal Agency customers of your company.

Existing Unique Federal Customers	Program Owner P
-----------------------------------	-----------------

[illegible]

[illegible]

Customers Worksheet

ur Cloud Service Offering being proposed for JAB Prioritization. This list should NOT include

[illegible]

[illegible]

clude all customers of the Cloud Service Provider. For (

[illegible]

(b) (6)

(202) 963-9254

(b) (6)

(b) (6), (b) (7)(C)

(b) (6)

7578648585

(b) (6)

[illegible]

example, if an agency is using an on premise

Contract Officer Point of Contact Name

(b) (6)

Shawn Roskosky

[illegible]

a version of your offering, or is using another offering, then they are not considered

[illegible]

[illegible]

ered current demand in this category. Similarly, if an agency is using a commer

[illegible]

[illegible]

cial version of your offering,

FISMA or FedRAMP ATO?

FEDRAMP

FEDRAMP ATO

FEDRAMP ATO - RMF 4

FEDRAMP ATO					
-------------	--	--	--	--	--

FEDRAMP ATO					
-------------	--	--	--	--	--

FEDRAMP ATO					
-------------	--	--	--	--	--

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

FEDRAMP ATO

[illegible]





Table 2: Proof of Demand from Indirect Customers Workshee

Instructions: List all CSP Customers with a FedRAMP ATO that use your serv

[illegible]

[illegible]

t

vice.

[illegible]

[illegible]

FedRAMP CSP Point of Contact E-mail

<Example: matt@goodrich.com >

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

[illegible]

[illegible]

[illegible]

<Example: FR1234567891>

[illegible]

Number of FedRAMP ATOs issued for the FedRAMP CSO	
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	0
2020	0
2021	0
2022	0
2023	0
2024	0
2025	0
2026	0
2027	0
2028	0
2029	0
2030	0
2031	0
2032	0
2033	0
2034	0
2035	0
2036	0
2037	0
2038	0
2039	0
2040	0
2041	0
2042	0
2043	0
2044	0
2045	0
2046	0
2047	0
2048	0
2049	0
2050	0
2051	0
2052	0
2053	0
2054	0
2055	0
2056	0
2057	0
2058	0
2059	0
2060	0
2061	0
2062	0
2063	0
2064	0
2065	0
2066	0
2067	0
2068	0
2069	0
2070	0
2071	0
2072	0
2073	0
2074	0
2075	0
2076	0
2077	0
2078	0
2079	0
2080	0
2081	0
2082	0
2083	0
2084	0
2085	0
2086	0
2087	0
2088	0
2089	0
2090	0
2091	0
2092	0
2093	0
2094	0
2095	0
2096	0
2097	0
2098	0
2099	0
2100	0
2101	0
2102	0
2103	0
2104	0
2105	0
2106	0
2107	0
2108	0
2109	0
2110	0
2111	0
2112	0
2113	0
2114	0
2115	0
2116	0
2117	0
2118	0
2119	0
2120	0
2121	0
2122	0
2123	0
2124	0
2125	0
2126	0
2127	0
2128	0
2129	0
2130	0
2131	0
2132	0
2133	0
2134	0
2135	0
2136	0
2137	0
2138	0
2139	0
2140	0
2141	0
2142	0
2143	0
2144	0
2145	0
2146	0
2147	0
2148	0
2149	0
2150	0
2151	0
2152	0
2153	0
2154	0
2155	0
2156	0
2157	0
2158	0
2159	0
2160	0
2161	0
2162	0
2163	0
2164	0
2165	0
2166	0
2167	0
2168	0
2169	0
2170	0
2171	0
2172	0
2173	0
2174	0
2175	0
2176	0
2177	0
2178	0

<Example: 24>

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

[illegible]

Instructions: List all current State, Local, Tribal, Territorial, Federally Funded

[illegible]

[illegible]

[illegible]

mers Worksheet

oposed for JAB Prioritization.

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Contract Officer Point of Contact E-mail

(b) (6) @LCRA.org

(b) (6) @nypa.gov

(b) (6) @njcourts.gov

(b) (6) @dir.texas.gov

(b) (6) @ladwp.com

(b) (6) @brookdalecc.edu

(b) (6) @llpower.org

(b) (6)@nypa.gov

(b) (5) @nypa.gov

@nypa.gov

@nypa.gov

@nypa.gov

(b) (6) @harlandale.net

[illegible]

[illegible]

[illegible]

[illegible]

Table 4: Proof of Potential Demand from Federal Agencies via RFIs, RFPs, and RFQs Worksheet

Instructions: List all Federal Agencies that have issued an RFI, RFs, or RFQ related to your cloud service that you have responded to in the last 18 months. The FedRAMP PMO reserves the right to request a copy of the RFI, RFP, or RFQ

Federal Agency Name	Name of RFI, RFP, or RFQ	RFI, RFP, or RFQ Number	Contract Point of Contact Name	Contract Point of Contact Title	Contract Point of Contact E-	Contract Point of	Release Date	Submission Date
DIR	Software Solutions Augmenting DIR-TSO-TMP-416	DIR-COPO-RFI-007	(b) (6)	Procurement Officer	(b) (6) @dir.texas.gov	NA	03/10/20	04/30/20
Golden Company - IC	SIGHBURGER	RFI-20-00091/BASE	(b) (6)	Contracting Officer	(b) (6) @tensleyconsulting.com	(b) (6)	12/18/2020	02/28/20
ARMY ARCYBER	RFQ Behavior Analytics	Direct Request	(b) (6)	Industry Engagement & Tech Assessment	(b) (6) @mail.mil	(b) (6)	03/01/20	05/15/20
ARMY PEO STI	Cyber Trident Cyber Training, Readiness, Integration,Delivery and Enter	Solicitation W900KK-20-R-0001	(b) (6)	Project Manager CT2	usarmy.oriando.peostri.list.pm-itts@mail.mil	(b) (6)	06/11/20	07/30/20
Air Force EITaaS	Enterprise IT as a Service	17-ITCC-044	(b) (6)	Contracting Officer	(b) (6) @us.af.mil	(b) (6)	5/24/2020	7/2/2020
Air Force SIBR	Small Business Innovation Phase II	J201-CS01	(b) (6)	Contracting Officer	(b) (6) @us.af.mil	(b) (6)	2/3/2020	6/15/2020
CENTCOM	GIDEON	classified	(b) (6)	Jacobs Engineering Corp.	(b) (6) @jacobs.com	(b) (6)	n/a - current contract	12/20/21
CENTCOM	AESOPS	classified	(b) (6)	Jacobs Engineering Corp.	(b) (6) @jacobs.com	(b) (6)	n/a - current contract	12/20/21
US Navy	ANTX		(b) (6)	BAH	@bah.com	(b) (6)	04/22	5/11/22
US Navy	ConMon		(b) (6)	BAH	@bah.com	(b) (6)	03/22	3/16/22
US Space Force	CYBERSECURITY AND DEFENSIVE CYBERSPACE OPERATION FOR SPACE MISSION SYSTEMS (DCO ACD)	Pre-RFP/eta 2024/recompete	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	05/24	07/24
US Air Force	614 AIR AND SPACE COMMUNICATIONS SQUADRON INFORMATION TECHNOLOGY SUPPORT (ACOMS IT)	Pre-RFP / FA461022RXXXX	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	07/22	09/22
US Air Force	ENTERPRISE CYBER CAPABILITIES (EC2)	Pre-RFP / FA877322R0005	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	07/22	09/22
US Air Force	Air Force Civil Engineer Control Systems Cyber Security Initiative	RFQ1550588	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	02/23	04/23
DHS CISA	ASSESSMENTS (Blue Team)	70RCSA21RFI000005	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	10/22	12/22
DHS CISA	ACTS	70QS0122R00000016	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	07/22	08/22
DOJ FBI	CEVA	classified	(b) (6)	Jacobos	@jacobs.com	(b) (6)	11/21	12/21
MPO	PURPLEFURY	classified	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	7/22	8/22
MPO	GOLDENGALLEON	classified	(b) (6)	Peraton	@mail.peraton.com	(b) (6)	9/22	10/22
DIA	ECST / SITEIII	classified	(b) (6)	Jacobs	@jacobs.com	(b) (6)	06/22	08/22

IronNet Collective Defense Post-Prioritization Notes - Ongoing

System Information

- System Name: IronNet Collective Defense
- POCs: (b) (6) @ironnet.com
- System Info: SaaS, Public Cloud, High
- [Business Case and Presentation](#)

Items to Track:

- Submitting full package: December 2023
- FedRAMP Ready: August/September 2023
- Submitted RAR: August 2023
- Prioritized: October 24, 2022

February 15, 2023

Attendees:

- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)

Notes:

- (b) (6) Quick update today, still making progress even if it has been slow. For starters, IronNet is going through a potential acquisition. Because of that, our work has slowed down until the terms of the agreement have been finalized. This should be 2 weeks to 2 months from now. With that said, we're still making good progress with the administration aspects of FR, gone through the controls, set the parameters, and the plan remains to have our product team make a hard effort in May, but we are on schedule.
- (b) (6) Yes, we have been concentrating on those controls, set the parameters, and right now we are making sure we have the correct answers in our SSP
- (b) (6) Great, so it sounds like everything is still moving towards the timeline we talked about last time: the RAR being submitted in August and the full package in December
- (b) (6) Our next meeting is April 19, but if you have any thoughts that with new ownership that there may be new goals and that might lead you away from getting a JAB authorization, just let me know
- (b) (6) No, they are enthusiastically supportive of our potential JAB authorization

Initial Post Prioritization Call

November 9, 2022

Attendees:

- (b) (6) - IronNet
 - GRC Director, project Mgr for FR initiative - Primary POC
 - (b) (6) @ironnetcybersecurity.com
- (b) (6) - IronNet
 - VP of Communications
- (b) (6) -IronNet
 - CIO/FR Lead for the company- Primary POC
 - (b) (6) @ironnetcybersecurity.com
- (b) (6) - IronNet
 - Public Sector Sales
- (b) (6) - IronNet
 - Product Management
- (b) (6) - PMO
- (b) (6) - PMO
- (b) (6) - PMO

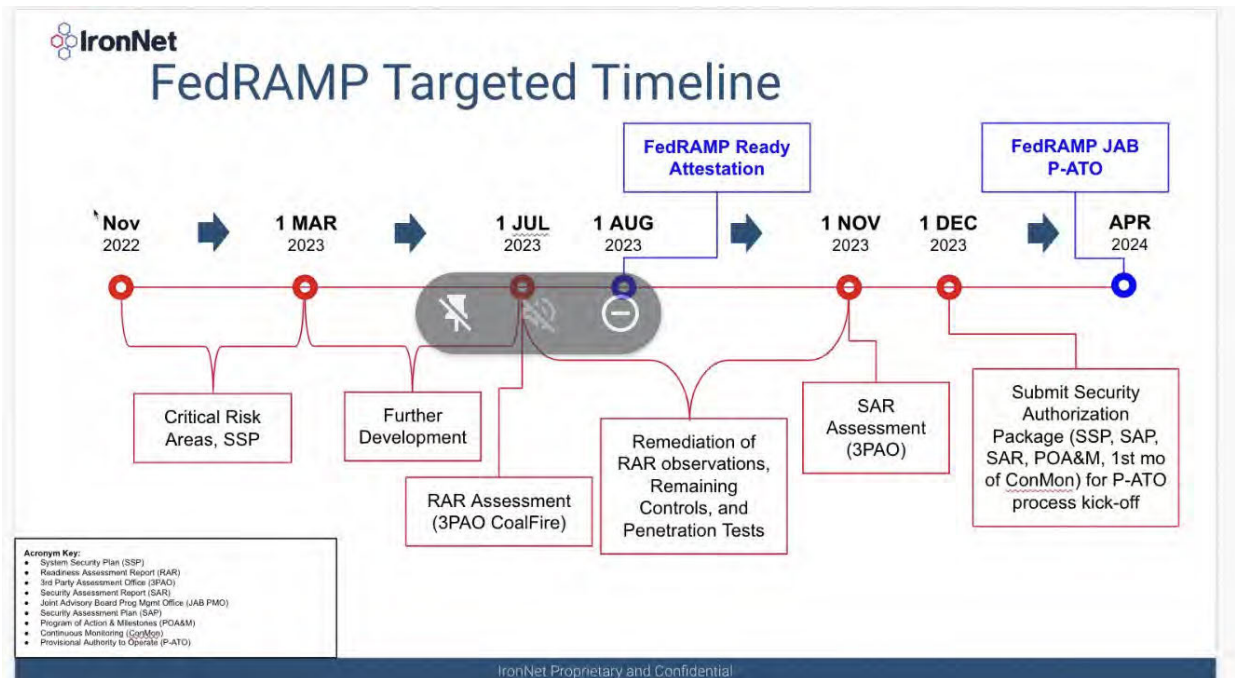
Agenda:

- Intros
- Overview of Process - show [JAB CSP Roles and Resp Process](#)
 - Next two phases:
 - Become FedRAMP Ready
 - Submit a full security package
 - It doesn't matter what round you were prioritized, whoever completes these two phases first, secures your spot in the kickoff order
 - The JAB can only be in process of an authorization with 3 CSPs at a time, so one of the reasons we'll meet regularly is to get timeline dates from each other, so neither of us have to wait/expect to kickoff but it takes longer
 - Once you kickoff, there is a go/no decision from the TR's and once you get the "go" decision, that's what put you in process on the Marketplace
 - If there is delay because of our lack of availability, you will not be penalized
- IronNet: Go/No go Decision- what does that look like?
 - Going over your entire security architecture (3 day meeting)
 - They will bring that back to the JAB reviewers to discuss- things were looking for- huge FIPS issues, etc.
 - If it's a "no" we will give you the list of "why" to get that fixed
 - You'll work with an authorization lead at some point once you're in the process and they will help with all of that- what to present, what to include, who should be

there to support you, etc. But usually we should catch this stuff in your RAR that is already submitted. This is also why we asked for your presentation in August, we were also looking for Red Flags then, so between that and your RAR, you should be good to go

- **JAB FedRAMP Ready and Security Package Submission Timeline**

- Is the timeline you presented back in August still accurate? What is your timeline right now for your expectation to submit a RAR to the PMO?
 - IronNet: No, there will have to be changes since then. There were significant changes that happened at IronNet, the market pressures caught up to us, and we had to do a significant restructuring. Our stock crashed hard, and hurt us in raising capital. But we are in the final phase of that restructuring, and we are almost back to where we need to be to be competitive. So, our workforce dropped significantly, but with that, we are committed to getting a FR high certification as quickly as we can. So, we would like to have a conversation around a possible timeline today
 - IronNet: Showed a new possible timeline with changes
 - Now- March 1: Critical Risk Areas
 - After March 1: Further development
 - July 1- RAR (still using Coalfire as our 3PAO)
 - This could be aggressive, and we may need a remediation period
 - Aug 1- To be FedRAMP Ready but could be 4-6 weeks longer)
 - Oct 1- Penetration Testing
 - Nov 1- SAR Assessment
 - Dec 1- Submit full package for the kick off process to begin
 - Changing the timeline is no problem, what we care about the most is transparency, so it's ok that the timeline is further out then predicted, being honest about that upfront helps both of us out the most. We just don't need to meet as regularly until March, and we just need you all to keep being transparent with us if other delays come up. Unless you ever tell us that you no longer want to go down the JAB route, we will not kick you out



• Next Steps and Meeting Cadence with the PMO

- Now that you're prioritized, you don't have to wait for our meetings, reach out to us anytime. However, it probably makes sense to meet again in mid-Feb and then start an every other month cadence from there. Once we are closer to your RAR submission, we can move to a monthly cadence. Then, when we are really close, we can meet every other week. How does that sound?

- IronNet: Agreed

- **ACTION:** (b) (6) to send the first meeting for the week of Feb 13 (afternoons work the best for IronNet because of their different time zones on the team)- DONE

• Press Release Guidance

- Press release will be live on the blog by the end of this month (if delayed, it will be communicated); once it is live, CSP can submit a press release to the PMO for approval.
 - Press release cannot say are JAB authorized, in-process with the JAB, not kicked off with the JAB, "first of a kind", FedRAMP Ready and no quotes from anyone in FedRAMP
 - Can announce you are prioritized to work with the JAB
- IronNet: Do we have a timeline of when we can send this out?
 - (b) (6) No, as long as we can see it first to review and approve, you can send it out whenever
- IronNet: Our next big milestone is being FR Ready, and I assume it's the same deal where we float it by you and then we're good?
 - (b) (6) Yes submit it to us first, but send it to Info@ so we have the record of that approval

- **Questions Regarding Relevant Guidance Documents**

- IronNet: The Boundary Guidance that you sent, when will the new changes be approved?
 - (b) (6) (b) (6) is working to remediate all of the comments as we speak, and then it has to go through a ton of approvals, so I cannot commit to a specific timeline. I don't think it will be before this calendar year, but we are hoping it will be in Q1/Q2 of 2023, so you can use that as guidance for your RAR

IronNet Collective Defense Post-Prioritization Notes - Ongoing

System Information

- System Name: IronNet Collective Defense
- POCs: (b) (6) @ironnet.com
- System Info: SaaS, Public Cloud, High
- [Business Case and Presentation](#)

Items to Track:

- Submitting full package: December 2023
- FedRAMP Ready: August/September 2023
- Submitted RAR: August 2023
- Prioritized: October 24, 2022

----- Initial Post Prioritization Call

November 9, 2022

Attendees:

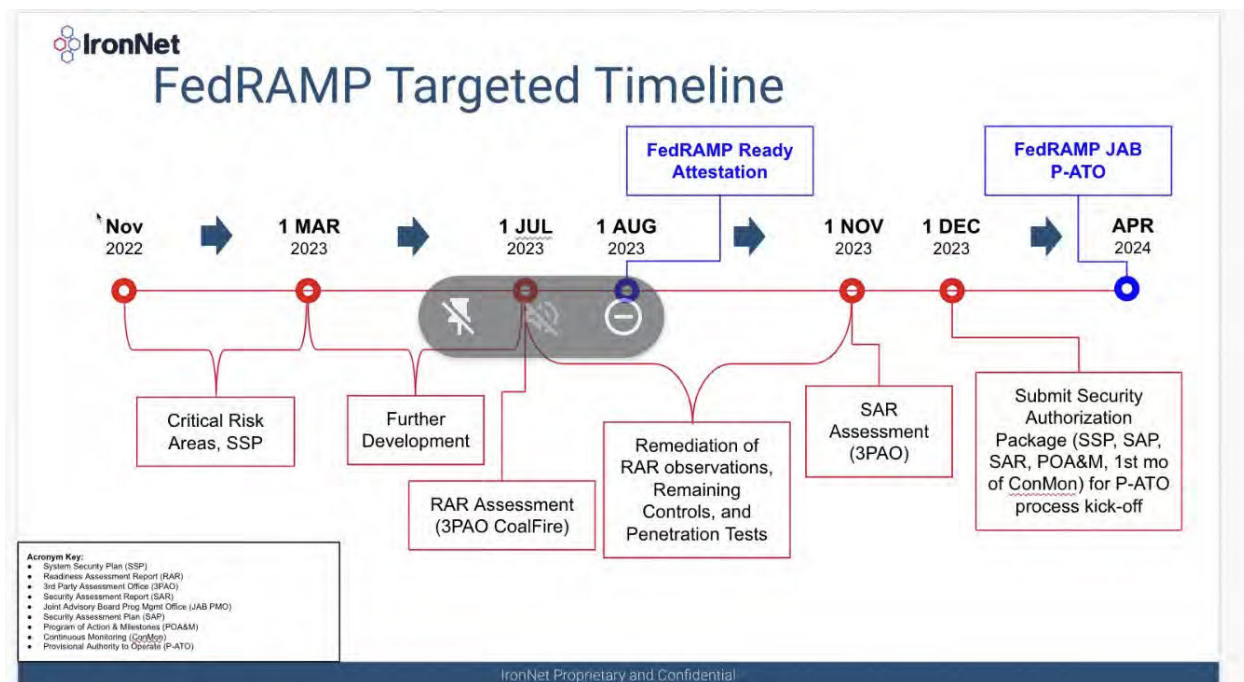
- (b) (6) - IronNet
 - GRC Director, project Mgr for FR initiative - Primary POC
 - (b) (6) @ironnetcybersecurity.com
- (b) (6) - IronNet
 - VP of Communications
- (b) (6) -IronNet
 - CIO/FR Lead for the company- Primary POC
 - (b) (6) @ironnetcybersecurity.com
- (b) (6) - IronNet
 - Public Sector Sales
- (b) (6) - IronNet
 - Product Management
- (b) (6) - PMO
- (b) (6) - PMO
- (b) (6) - PMO

Agenda:

- Intros
- Overview of Process - show [JAB CSP Roles and Resp Process](#)
 - Next two phases:
 - Become FedRAMP Ready
 - Submit a full security package

- It doesn't matter what round you were prioritized, whoever completes these two phases first, secures your spot in the kickoff order
 - The JAB can only be in process of an authorization with 3 CSPs at a time, so one of the reasons we'll meet regularly is to get timeline dates from each other, so neither of us have to wait/expect to kickoff but it takes longer
 - Once you kickoff, there is a go/no decision from the TR's and once you get the "go" decision, that's what put you in process on the Marketplace
 - If there is delay because of our lack of availability, you will not be penalized
- IronNet: Go/No go Decision- what does that look like?
 - Going over your entire security architecture (3 day meeting)
 - They will bring that back to the JAB reviewers to discuss- things were looking for- huge FIPS issues, etc.
 - If it's a "no" we will give you the list of "why" to get that fixed
 - You'll work with an authorization lead at some point once you're in the process and they will help with all of that- what to present, what to include, who should be there to support you, etc. But usually we should catch this stuff in your RAR that is already submitted. This is also why we asked for your presentation in August, we were also looking for Red Flags then, so between that and your RAR, you should be good to go
- **JAB FedRAMP Ready and Security Package Submission Timeline**
 - Is the timeline you presented back in August still accurate? What is your timeline right now for your expectation to submit a RAR to the PMO?
 - IronNet: No, there will have to be changes since then. There were significant changes that happened at IronNet, the market pressures caught up to us, and we had to do a significant restructuring. Our stock crashed hard, and hurt us in raising capital. But we are in the final phase of that restructuring, and we are almost back to where we need to be to be competitive. So, our workforce dropped significantly, but with that, we are committed to getting a FR high certification as quickly as we can. So, we would like to have a conversation around a possible timeline today
 - IronNet: Showed a new possible timeline with changes
 - Now- March 1: Critical Risk Areas
 - After March 1: Further development
 - July 1- RAR (still using Coalfire as our 3PAO)
 - This could be aggressive, and we may need a remediation period
 - Aug 1- To be FedRAMP Ready but could be 4-6 weeks longer)
 - Oct 1- Penetration Testing
 - Nov 1- SAR Assessment
 - Dec 1- Submit full package for the kick off process to begin
 - Changing the timeline is no problem, what we care about the most is transparency, so it's ok that the timeline is further out then predicted, being honest about that upfront helps both of us out the most. We just don't need to meet as regularly until March, and we just need you all to

keep being transparent with us if other delays come up. Unless you ever tell us that you no longer want to go down the JAB route, we will not kick you out



• Next Steps and Meeting Cadence with the PMO

- Now that you're prioritized, you don't have to wait for our meetings, reach out to us anytime. However, it probably makes sense to meet again in mid-Feb and then start an every other month cadence from there. Once we are closer to your RAR submission, we can move to a monthly cadence. Then, when we are really close, we can meet every other week. How does that sound?

- IronNet: Agreed

- **ACTION: Claire/Megan to send the first meeting for the week of Feb 13 (afternoons work the best for IronNet because of their different time zones on the team)- DONE**

• Press Release Guidance

- Press release will be live on the blog by the end of this month (if delayed, it will be communicated); once it is live, CSP can submit a press release to the PMO for approval.
 - Press release cannot say are JAB authorized, in-process with the JAB, not kicked off with the JAB, "first of a kind", FedRAMP Ready and no quotes from anyone in FedRAMP
 - Can announce you are prioritized to work with the JAB
- IronNet: Do we have a timeline of when we can send this out?

- (b) (6) No, as long as we can see it first to review and approve, you can send it out whenever
 - IronNet: Our next big milestone is being FR Ready, and I assume it's the same deal where we float it by you and then we're good?
 - (b) (6) Yes submit it to us first, but send it to Info@ so we have the record of that approval
- **Questions Regarding Relevant Guidance Documents**
 - IronNet: The Boundary Guidance that you sent, when will the new changes be approved?
 - (b) (6) (b) (6) is working to remediate all of the comments as we speak, and then it has to go through a ton of approvals, so I cannot commit to a specific timeline. I don't think it will be before this calendar year, but we are hoping it will be in Q1/Q2 of 2023, so you can use that as guidance for your RAR



12 messages

Mon, Jul 27, 2020 at 12:55 PM

(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @ironnetcybersecurity.com>, (b) (6) <(b) (6) @kratosdefense.com>, (b) (6) @gsa.gov, (b) (6) @gsa.gov, john.hamilton@gsa.gov

(b) (5)

I hope you are doing well. The IronNet 3PAO resubmitted our RAR on July 22 in [MAX.GOV](#). Can you confirm that you received it and it has been put in the queue for review? I would like to give my senior leadership an update on the status. Thank you!

(b) (5)

IronNet Cybersecurity Inc.
8135 Maple Lawn Blvd., Suite 455
Fulton, MD 20759
Phone: (b) (6) [REDACTED]
(b) (6) [REDACTED] @ironnetcybersecurity.com

This message is intended exclusively for the individual(s) or entity to which it is addressed. It may contain information that is privileged or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Any digital signatures or certifications transmitted with this email are for sender verification purposes only and have not been included in this email for the purposes of binding the company to any statement or attachment made herein or for any other purpose.

Mon, Jul 27, 2020 at 1:06 PM

Hamilton - QQC <john.hamilton@gsa.gov>

(b) (5)

(b) (6) is out of the office today, however, your RAR came to the Review Team and was added to our queue on July 23. Our reviewer has already reviewed it and provided minor clarification comments to your 3PAO. Please feel free to inquire to your 3PAO for status on his update.

(b) (6) -- please ensure to advise the PMO team on your resubmission (cc'd above); (b) (6) is out of office at this time.

Best

(b) (8)

Best.

(b) (5)

[Quoted text hidden]

11

(b) (6)

(b) (6) @gsa.gov



www.FedRAMP.gov

Mon, Jul 27, 2020 at 1:11 PM
 (b) (6) <(b) (6)@ironnetcybersecurity.com>
 To: (b) (6) - QQC-C <(b) (6)@gsa.gov>
 Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@kratosdefense.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>, William Hamilton - QQC <john.hamilton@gsa.gov>

[Quoted text hidden]

[Quoted text hidden]

(b) (6) <(b) (6) @kratosdefense.com> Mon, Jul 27, 2020 at 1:23 PM
 To: (b) (6) <(b) (6) @ironnetcybersecurity.com>; "(b) (6) @gsa.gov" <(b) (6) @gsa.gov>
 Cc: (b) (6) <(b) (6) @ironnetcybersecurity.com>; <(b) (6) @ironnetcybersecurity.com>; "(b) (6) @gsa.gov" <(b) (6) @gsa.gov>; "(b) (6) @ironnetcybersecurity.com" <(b) (6) @ironnetcybersecurity.com>; "(b) (6) @gsa.gov" <(b) (6) @gsa.gov>; "(b) (6) @ironnetcybersecurity.com" <(b) (6) @ironnetcybersecurity.com>; "(b) (6) @ironnetcybersecurity.com>; "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>; (b) (6) <(b) (6) @kratosdefense.com>

Laurie and I chatted 7/24/2020 with two minor items. The documentation on MAX.gov reflects our discussions and FedRAMP PMO possess the most current version.

Please let me know if there are questions.

Sincerely, (b) (6)

Kratos | Chandler, AZ | TTS-Cyber Principal Security Consultant

C: (b) (6) | www.kratosdefense.com



[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]
[Quoted text hidden]



[Quoted text hidden]

(b) (6) <(b) (6)@ironnetcybersecurity.com> Mon, Jul 27, 2020 at 1:25 PM
 To: (b) (6) <(b) (6)@kratosdefense.com>
 Cc: (b) (6) <(b) (6)@kratosdefense.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>
 <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov> <(b) (6)@gsa.gov>,
 (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov>
 <(b) (6)@gsa.gov>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6) <(b) (6)@gsa.gov>
 <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>

Thanks (b) (6)

[Quoted text hidden]

(b) (6) - QQC-C (b) (6) <(b) (6)@gsa.gov> Mon, Jul 27, 2020 at 1:26 PM
 To: (b) (6) <(b) (6)@kratosdefense.com>
 Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>
 <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov> <(b) (6)@gsa.gov>,
 (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov>
 <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>,
 "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6) <(b) (6)@kratosdefense.com>

Thanks, Jim. We will get eyes on updates.

(b) (6)

On Mon, Jul 27, 2020 at 1:23 PM (b) (6) <(b) (6)@kratosdefense.com> wrote:

[Quoted text hidden]

--
[Quoted text hidden]



(b) (6) - QQC-C (b) (6) <(b) (6)@gsa.gov> Tue, Jul 28, 2020 at 3:08 PM
 To: (b) (6) <(b) (6)@kratosdefense.com>
 Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@ironnetcybersecurity.com>
 <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov> <(b) (6)@gsa.gov>,
 (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov>
 <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>,
 "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6) <(b) (6)@kratosdefense.com>

<https://mail.google.com/mail/u/0/?ik=e8a7f9c7cf&view=pt&search=all&permthid=thread-f:1673389914226316183&simpl=msg-f:1673389914226316183&simpl=m...> 4/7

To: (b) (6) <(b) (6)@kratosdefense.com>
Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>,
(b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov>
<(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>,
(b) (6) <(b) (6)@gsa.gov> <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>
<(b) (6)@ironnetcybersecurity.com>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6)
<(b) (6)@kratosdefense.com>

Your dates/version #s will need to be the same on all, so since you will need to update, you will need a new PDF too.

Best.

(b) (6)

[Quoted text hidden]

[Quoted text hidden]



FedRAMP | TTS | GSA
www.FedRAMP.gov

(b) (6) Tue, Jul 28, 2020 at 3:30 PM
 To: (b) (6) <(b) (6)@kratosdefense.com>
 (b) (6) <(b) (6)@gsa.gov> <(b) (6)@gsa.gov>
 Cc: (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>,
 (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>, (b) (6) <(b) (6)@gsa.gov>
 <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com> <(b) (6)@ironnetcybersecurity.com>,
 (b) (6) <(b) (6)@gsa.gov> <(b) (6)@gsa.gov>, (b) (6) <(b) (6)@ironnetcybersecurity.com>
 <(b) (6)@ironnetcybersecurity.com>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6)
 <(b) (6)@kratosdefense.com>

Tue, Jul 28, 2020 at 3:35 PM

Thank you, Will change everything to today's date, re-PDF and sign. I will have both a Word – tracked version with 7/24 review, Word final version with changes accepted, and PDF final version with today's dates. Three (3) total documents.

[Quoted text hidden]

[Quoted text hidden]



(b) (6) <(b) (6)@kratosdefense.com>
 To: (b) (6) @gsa.gov" <(b) (6)@gsa.gov>
 Cc: (b) (6) @ironnetcybersecurity.com" <(b) (6)@ironnetcybersecurity.com>,
 (b) (6) @ironnetcybersecurity.com" <(b) (6)@ironnetcybersecurity.com>, (b) (6) @gsa.gov"
 <(b) (6)@gsa.gov>, (b) (6)@ironnetcybersecurity.com" <(b) (6)@ironnetcybersecurity.com>,
 (b) (6) @gsa.gov" <(b) (6)@gsa.gov>, (b) (6)@ironnetcybersecurity.com"
 (b) (6)@ironnetcybersecurity.com>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6)
 <(b) (6)@kratosdefense.com>

Tue, Jul 28, 2020 at 3:59 PM

Please let me know if there are questions.

Sincerely, (b) (6)

C: (b) (6) | www.kratosdefense.com

KRATOS

[Quoted text hidden]



(b) (6) - QQC-C (b) (6) @gsa.gov>
 To: (b) (6) <(b) (6) @kratosdefense.com>
 Cc: (b) (6) @ironnetcybersecurity.com" <(b) (6) @ironnetcybersecurity.com>,
 (b) (6) @ironnetcybersecurity.com" <(b) (6) @ironnetcybersecurity.com>, (b) (6) @gsa.gov"
 <(b) (6) @gsa.gov>, (b) (6) @ironnetcybersecurity.com" <(b) (6) @ironnetcybersecurity.com>,
 (b) (6) @gsa.gov" <(b) (6) @gsa.gov>, (b) (6) @ironnetcybersecurity.com"
 <(b) (6) @ironnetcybersecurity.com>, "john.hamilton@gsa.gov" <john.hamilton@gsa.gov>, (b) (6)
 <(b) (6) @kratosdefense.com>

Wed, Jul 29, 2020 at 9:37 AM

(b) (6)

[Quoted text hidden]



FedRAMP | TTS | GSA
www.FedRAMP.gov



William Hamilton - QQC <william.hamilton@gsa.gov>

IronNet Cybersecurity inc., IronCloud -- Recommending FRR - Agency ATO only

3 messages

(b) (6) - QQC-C (b) (6) @gsa.gov> Wed, Jul 29, 2020 at 12:38 PM
 To: William Hamilton - QQC <william.hamilton@gsa.gov>
 Cc: Ashley Mahan - XAAB <ashley.mahan@gsa.gov>, (b) (6) - QQC-C (b) (6) @gsa.gov>, (b) (6) - QQC-C (b) (6) @gsa.gov>, (b) (6) - QQC-C (b) (6) @gsa.gov>, (b) (6) - QQC-C (b) (6) @gsa.gov>, (b) (6) - QQC-C (b) (6) @gsa.gov>, (b) (6) - QQC-C (b) (6) @gsa.gov>, Ryan Hoelsing - QQC <ryan.hoelsing@gsa.gov>

Hi John -- The 3PAO addressed our concerns raised regarding the IronNet RAR and it's in good shape. The CSP has some documentation matters to address and they use several external services, but that's about it. They really had their hearts set on JAB path, but Agency Engagement and JAB members met with them to appropriately manage expectations.

Attached please find our RAR Evaluation Rep and Director's letter draft. RAR Eval Exec Summary notes are below as well.

Please advise if you have any questions or concerns, or please recommend for Ashley's approval.

Best,
 (b) (6)

IronNet RAR Eval PDF: (b) (6)

IronNet RAR Eval GoogleSheet: (b) (6)

Director's letter: (b) (6)

Eval Rep Executive Summary notes:

Based on this RAR evaluation, the FedRAMP PMO has determined that this **Government Only Community** cloud service offering is FedRAMP Ready.

Agencies considering use of IronCloud should consider the following items of note:

1. Use of External Services Lacking FedRAMP Authorization: FedRAMP encourages use of FedRAMP Authorized services*, where possible. The RAR indicates that IronNet uses several third party providers and external services/systems lacking FedRAMP authorization (at time of RAR) to support IronCloud (for example, **Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, Whols [API]**). The RAR describes external leveraged services and associated risks. The information provided in the RAR is intended to help Agencies in determining suitability of using the service based on each Agency's risk tolerance. Agencies must understand that use of services that have not been FedRAMP-authorized represent unknown risk and have not been validated by a 3PAO. Agencies must understand how their data is interacting with such services, and must assess and accept risk for use of these external services, especially those services that provide critical security functionality. Agencies are encouraged to engage the CSP about questions concerning use of the external services and may involve FedRAMP PMO in such discussions, as desired.
2. Policies and Procedures: The CSP has a complete set of policies and procedures but the 3PAO notes that some of the documents have some deficiencies that are being updated. Policies and Procedures should be updated and finalized for the initial Full Assessment.
3. SSP Completion: SSP is 50% developed with an "overall operational maturity sufficient to satisfy FedRAMP requirements". SSP should be finalized prior to the initial Full Assessment.
4. Not applicable and Alternative Implementation controls: 8 N/A and 5 Alternative Implementation controls should be fully validated during the initial Full Assessment.

As part of risk-based authorization and use decisions, Agencies are reminded to also review associated leveraged service authorization package(s), such as for the underlying Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), for full awareness of risks associated with using a cloud service.

*Note: Under most circumstances, the use of external services that lack FedRAMP Agency Authorization or Joint Authorization Board (JAB) Provisional Authorization (P-ATO) is permitted only if you are pursuing Agency Authorization, and if the partnering Agency accepts risk. The JAB requirements related to external services are much more stringent; if

interested in pursuing a JAB P-ATO, please inquire to info@fedramp.gov if you use any external services other than those with JAB P-ATO.

CSP POCs:

(b) (6) President (b) (6) (b) (6)@castus.tv

(b) (6) (b) (6)@ironnetcybersecurity.com

(b) (6) Sales (b) (6) (b) (6)@castus.tv

(b) (6)@ironnetcybersecurity.com

(b) (6) <(b) (6)@ironnetcybersecurity.com>,

(b) (6) <(b) (6)@ironnetcybersecurity.com>,

(b) (6) <(b) (6)@ironnetcybersecurity.com>,

3PAO Assessor: Kratos

(b) (6) (b) (6)@kratosdefense.com

--

(b) (6)
FedRAMP PMO Support, Agency Review Team Lead
(b) (6)@gsa.gov



FedRAMP | TTS | GSA
www.FedRAMP.gov

John Hamilton <william.hamilton@gsa.gov>

Wed, Jul 29, 2020 at 2:27 PM

To: (b) (6) - QQC-C <(b) (6)@gsa.gov>

Cc: Ashley Mahan - XAAB <ashley.mahan@gsa.gov>, (b) (6) - QQC-C (b) (6)@gsa.gov, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, Ryan Hoelsing - QQC <ryan.hoelsing@gsa.gov>

(b) (6) - After reviewing the team's RAR evaluation, I also think they're in good shape and meeting the vast majority of the requirements; there is some additional documentation work needed by the CSP (i.e., completing their SSP and policies and procedures) and their 3PAO will need to re-evaluate a number of N/A / alternative implementation controls during the full assessment.

Ashley - I'm also recommending for FedRAMP Ready; thanks all!

~John

[Quoted text hidden]

--

John Hamilton
FedRAMP Program Manager of Security Operations
Technology Transformation Service | GSA
202.394.2812 | william.hamilton@gsa.gov

2 attachments



Cc: (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, (b) (6) - QQC-C <(b) (6)@gsa.gov>, Ryan Hoelsing - QQC <ryan.hoelsing@gsa.gov>

website: www.fedramp.gov

<https://mail.google.com/mail/u/0/?ik=e8a7f9c7cf&view=pt&search=all&permthid=thread-f:1673569979993534748&simpl=msg-f:1673569979993534748&simpl=m...> 3/3



To: (b) (6)
President
IronNet Cybersecurity Inc.

7/29/2020

From: Ashley Mahan
FedRAMP Director
General Services Administration

Re: IronNet IronCloud FedRAMP Ready Approval - Agency Authorization Only

(b) (6)

The FedRAMP PMO has completed evaluation of the IronNet IronCloud Readiness Assessment Report (RAR) provided by Kratos. Based on the outcome of the RAR evaluation, the cloud service offering (CSO) has been approved as FedRAMP Ready for Agency Authorization.

The FedRAMP PMO recognizes the CSO is still maturing documentation and capabilities such as updating the control family policies and procedures and system security plan (SSP). The FedRAMP PMO also recognizes that the CSO uses several third party providers and external services/systems lacking FedRAMP Authorization (at time of RAR) to support IronCloud (i.e., **Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, and Whois (API)**). Potential agency partners pursuing a FedRAMP Agency Authorization must accept risk for this use, since these services are not FedRAMP Authorized.

The FedRAMP PMO relies on you to ensure the security posture of your service offering protects federal agency data and for you to work closely with any potential agency(ies) to ensure they understand how their data will be protected in your environment. For example, in cases where several multi-factor authentication methods are provided by a service, cloud service providers (CSPs) must identify which methods of multi-factor access are/are not FIPS 140-2 validated, and encourage customers and partners to use methods that are FIPS validated.

We look forward to continue working with you as you pursue a FedRAMP Agency Authorization.

Please don't hesitate to reach out if you have any questions.

Sincerely,

Ashley Mahan
FedRAMP Director

Readiness Assessment Report (RAR) Evaluation Report

FR2020139614

FedRAMP Review for:	IronNet Cybersecurity Inc., IronCloud			System Categorization:	Moderate
Recommendation:	FedRAMP Ready - Agency Auth. Only			Deployment Model:	Govt Only Comm.
RAR Date:	7/28/2020	Ver.	1.3	Service Model:	SaaS
FedRAMP Evaluation Date:	7/28/2020			Recommended by 3PAO?	Yes
Signed?	Yes			3PAO Name:	Kratos

Section A: Executive Summary

The purpose of this report is to summarize the evaluation of Kratos' review of IronNet Cybersecurity Inc., IronCloud for consideration of the "FedRAMP Ready" designation. The evaluation of the Readiness Assessment Report (RAR) was conducted by the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO). The intended audiences for this report are agencies considering using the service offering, the Cloud Service Provider (CSP), and the Third Party Assessment Organization (3PAO).

Based on this RAR evaluation, the FedRAMP PMO has determined that this **Government Only Community** cloud service offering is FedRAMP Ready.

Agencies considering use of IronCloud should consider the following items of note:

1. Use of External Services Lacking FedRAMP Authorization: FedRAMP encourages use of FedRAMP Authorized services*, where possible. The RAR indicates that IronNet uses several third party providers and external services/systems lacking FedRAMP Authorization (at time of RAR) to support IronCloud (e.g., **Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, and Whois [API]**). The RAR describes external leveraged services and associated risks. The information provided in the RAR is intended to help agencies in determining the suitability of using the service based on each agency's risk tolerance. Agencies must understand that the use of services, that have not been FedRAMP Authorized, represent unknown risk and have not been validated by a 3PAO. Agencies must understand how their data is interacting with such services, and must assess and accept risk for the use of these external services, especially those services that provide critical security functionality. Agencies are encouraged to engage the CSP about questions concerning the use of the external services and may involve the FedRAMP PMO in such discussions, as desired.

2. Policies and Procedures: The CSP has a complete set of policies and procedures, but the 3PAO notes that some of the documents have some deficiencies that are being updated.

CSP Action: The policies and procedures should be updated and finalized prior to the initial full assessment.

3. SSP Completion: The SSP is 50% developed with an "overall operational maturity sufficient to satisfy FedRAMP requirements".

CSP Action: The SSP should be finalized prior to the initial full assessment.

4. Not applicable and Alternative Implementation controls: 8 controls are designated as N/A and 5 controls are designated as alternative implementations.

3PAO Action: These controls should be fully validated during the initial full assessment.

As part of risk-based authorization and use decisions, agencies are reminded to also review associated leveraged service authorization package(s), such as for the underlying Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), for full awareness of risks associated with using a cloud service.

*Note: Under most circumstances, the use of external services that lack FedRAMP Agency Authorization or Joint Authorization Board (JAB) Provisional Authorization (P-ATO) is permitted only if you are pursuing Agency Authorization, and if the initial partnering agency accepts risk. The JAB requirements related to external services are much more stringent; if interested in pursuing a JAB P-ATO, please inquire to info@fedramp.gov if you use any external services other than those with a JAB P-ATO.

Key:

Concern = May require CSP Action for FRR or FR Authorization.

OK = No necessary action for FedRAMP Ready to be granted.

N/A = Not applicable for this service.

Section B: RAR Attestation Statement & Executive Summary

#	Description	OK/Concern	Comments
1	Do the Readiness Assessment Activities within the Attestation section provide the date(s) and location(s) of the Readiness Assessment and a description of the 3PAO's activities?	Ok	
2	Does the Executive Summary provide an adequate description of the system?	Ok	
3	Does the Executive Summary provide an adequate overview of information/findings provided in Sections 4.1, 4.2, and 4.3, including notable strengths and other areas for consideration?	Ok	
4	Has 3PAO adhered to the numbered list of instructions in Section 2.2?	Ok	

Section C: CSP System Information (addresses RAR Section 3)

#	Description	OK/Concern	Comments
1	Is the CSP system information within Table 3-1 complete? (Section 3.0)	Ok	

Readiness Assessment Report (RAR) Evaluation Report

FR2020139614

2	Has the RAR indicated that the 3PAO has performed a full validation of the authorization boundary? (Section 3.1)	Ok	
3	In addition to a boundary diagram, has the RAR provided a written description that clearly and accurately describes the authorization boundary? (Section 3.1)	Ok	
4	Are the leveraged services clearly defined, explained and adequate? (Section 3.2 Table 3-2)	Ok	<i>AWS GovCloud, Google Services (Google Cloud Platform Products and underlying Infrastructure)</i>
5	Are all external systems and services noted in adequate detail? (Section 3.3 Table 3-3)	Ok	<i>Google Cloud Identity, IronSensor, Customer Log SIEM or SOAR, Domain Tools, TOR Project, Umbrella, Majestic Million, and Whois (API)</i>
6	Are all APIs that are used to push, pull, or exchange data and information with external resources listed and described? (Section 3.4 Table 3-4)	Ok	
7	Are the system's TIC capabilities clearly documented? (Section 3.5)	Ok	
8	Has the RAR indicated that the 3PAO has performed a full validation of the Data Flow Diagram(s)? (Section 3.6)	Ok	
9	In addition to the data flow diagrams, has the RAR provided a written description that adequately identifies and delineates the data flows (i.e., including how data enters and exits a system)? (Section 3.6)	Ok	
10	Does the RAR demonstrate solid separation measures used by the CSP? (Section 3.7)	Ok	

Section D: Capability Readiness (addresses RAR Sections 4.1 and 4.2)

#	Description	OK/Concern	Comments
1	Does the RAR adequately address all Federal Mandates? (Table 4-1)	Ok	
2	Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? (Section 4.2.1 and Table 4-2)	Ok	
4	Does the system properly describe and clarify its adherence to current Digital Identity requirements for Identification, Authentication, and Access controls in accordance with NIST SP 800-63 r3? (Section 4.2.3 and Table 4-4)	Ok	
5	Does the RAR show the system has consistent audit, alerting, malware, and incident response controls in place? (Section 4.2.4 and Table 4-5)	Ok	
6	Does the RAR indicate consistent contingency planning and disaster recovery controls in place? (Section 4.2.5 and Table 4-6)	Ok	
7	Does the CSP demonstrate consistent configuration and risk management controls? Specifically, are authenticated scans performed monthly on OS/ Infrastructure and Web and Database applications, as applicable? Are vulnerabilities remediated within the required timeframes? (Section 4.2.6 and Table 4-7)	Ok	

Readiness Assessment Report (RAR) Evaluation Report

FR2020139614

8	Does the RAR illustrate that the CSP has consistent data center security? (Section 4.2.7 and Table 4-8)	Ok	
9	Does the RAR indicate that the CSP has a complete set of policies and procedures? (Section 4.2.8 and Table 4-9)	Ok	<p><i>The CSP has a complete set of policies and procedures, but the 3PAO notes that some of the documents have some deficiencies. IronNet is working with a trusted advisor to update these documents and the 3PAO states that these will be "finalized, approved, and signed within 90 days of receiving FedRAMP Ready status and before the formal FedRAMP assessment has begun."</i></p> <p><i>CSP Action: The policies and procedures should be updated and finalized prior to the initial full assessment.</i></p>
10	Does the RAR indicate that the CSP has adequate security awareness and role-based training? (Section 4.2.8 and Table 4-11)	Ok	

Section E: Additional Capability Information (addresses RAR Section 4.3)

#	Description	OK/Concern	Comments
1	Does the RAR indicate that the CSP is adequately staffed? (Section 4.3.1 and Table 4-12)	Ok	
2	Does the RAR indicate a mature Change Management Capability? (Section 4.3.2 and Table 4-13)	Ok	
3	Does the RAR show that CSP vendor dependencies and related agreements are adequately maintained? (Section 4.3.3 and Tables 4-14, 4-15, and 4-16)	Ok	
4	Does the RAR indicate that the CSP has adequate Continuous Monitoring? (Section 4.3.4 and Tables 4-17 & 4-18)	Ok	
5	Does the RAR document the SSP maturity level? (Section 4.3.5 and Table 4-19)	Ok	<p><i>The SSP is 50% developed with an "overall operational maturity sufficient to satisfy FedRAMP requirements".</i></p> <p><i>CSP Action: The SSP should be finalized prior to the initial full assessment.</i></p>
6	Does RAR document all controls currently designated "Not Applicable"? (Section 4.3.5, Table 4-20)	Ok	<p><i>8 controls are currently designated as "N/A", but the 3PAO disagrees with AC-19(5), PS-3(3), SC-15, and SC-18.</i></p> <p><i>3PAO Action: Please validate the status of these controls during the initial full assessment.</i></p>
7	Does RAR document all controls currently designated "Alternative Implementation"? (Section 4.3.5, Table 4-21)	Ok	<p><i>5 controls have alternative implementations, but the 3PAO disagrees with AC-19, CP-8, CP-8(1), and CP-8(2).</i></p> <p><i>3PAO Action: Please validate the status of these controls prior to the initial full assessment.</i></p>

v2.4

Section F: Additional Comments

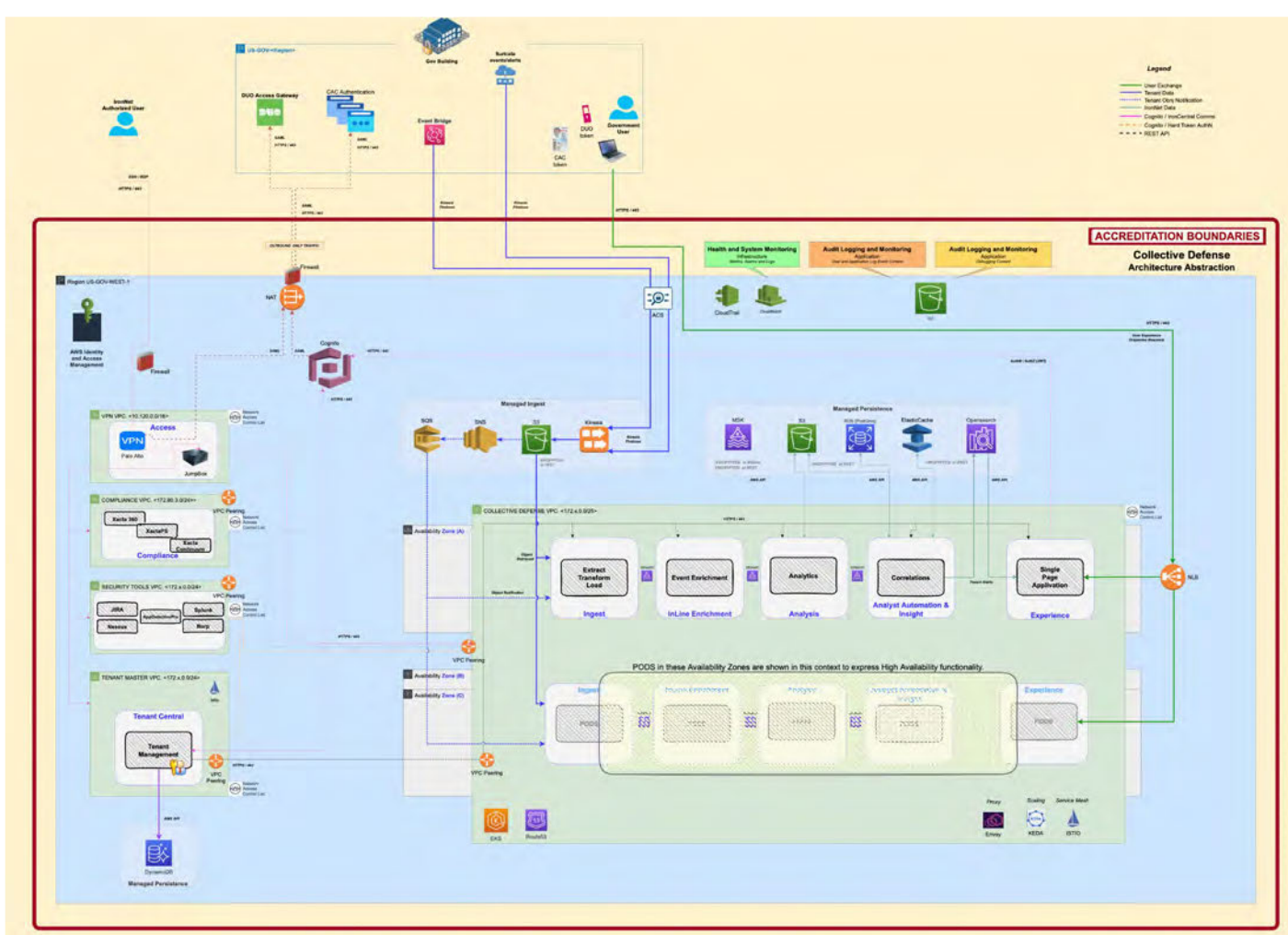


IronNet Collective Defense

Presentation to the FedRAMP PMO

10 August 2022

Authorization Boundary Diagram



FedRAMP High External Services

- **CloudTrail** - monitors & records account activity across AWS infrastructure
- **CloudWatch** - collects monitoring and operational data (e.g., logs, metrics)
- **Cognito** - federated identity service
- **DynamoDB** - NoSQL database service for key-value and document data
- **Elastic Kubernetes Service (EKS)** - managed container orchestration
- **Identity and Access Management (IAM)** - AWS authentication/authorization
- **Kinesis Data Firehose** - extract, transform, and load (ETL) service
- **Managed Streaming for Kafka (MSK)** - distributed event streaming service

FedRAMP High External Services

- **Network Address Translation (NAT)** - unidirectional connection service
- **Network Load Balancer (NLB)** - AWS request distribution service
- **OpenSearch** - AWS search service
- **Relational Database Service (RDS)** - AWS service for Postgres databases
- **Route53** - Domain Name System (DNS) service providing DNSSEC
- **Simple Storage Service (Amazon S3)** - main data store for IronDefense
- **Simple Notification Service (Amazon SNS)** - service used for messaging
- **Simple Queue Service (Amazon SQS)** - manages SNS notifications
- **Virtual Private Cloud (VPC) Peering** - allows private routing between VPCs

External Connections

System/Service	Protocol/Port
SAML	HTTPS/443
Jump Host	SSH/22 RDP/3389 (Windows)
Customer User Access	HTTPS/443
Event Bridge/Kinesis Firehose	HTTPS/443
Suricata/Kinesis Firehose	HTTPS/443

VPC Interconnections

Name	Region	IPs Region	Description
Default West VPC	GovCloud West	No IPs	Default VPC (unused) - No inbound or outbound rules
Security Tools	GovCloud West	172.73.0.0/24 100.0.0.0/16	Hosts security tools e.g. Jira, Nessus, etc...
VPN	GovCloud West	10.120.0.0/16	Hosts Palo Alto FW and VPN
Compliance	GovCloud West	172.80.3.0/24 172.80.4.0/24	Hosts Xacta compliance tools
Tenant Master VPC	GovCloud West	172.x.0.0/24	Tenant Management/Access Control
Collective Defense VPC	GovCloud West	172.x.0.0/25	Product Platform, processes customer network traffic and cloud service provider logs

VPC Interconnections (cont.)

Destination VPC	Source VPC	Port / Protocol	Description
Security Tools	VPN	8000 / TCP	Web UI for VPN users
Security Tools	VPN	554 / TCP 443 / TCP	Splunk web UI for VPN users on 192.168.252.0/24
Security Tools	VPN	9997 / TCP	Forwards to the Splunk indexer
Security Tools	VPN	8000 / TCP	Splunk Search page clients
Security Tools	VPN	22 / TCP	SSH access for VPN users to administer Splunk
Security Tools	VPN	8084 / TCP	Collect data from defenders to the console from VPCs connected to transit gateway
Security Tools	n/a	8088 / TCP	VPC Firehouse and Kinesis to collect VPC logs into Splunk from 18.253.138.192/26
Security Tools	Transit gateway	5432 / TCP	Xacta Postgres DB server

VPC Interconnections (cont.)

Destination VPC	Source VPC	Port / Protocol	Description
Security Tools	VPN	8081 / TCP 8083 / TCP	Prisma cloud compute Twistlock Rest API from VPCs connected to the transit gateway
Security Tools	VPN	5432 / TCP	Xacta Postgres DB server
Security Tools	VPN	22 / TCP	SSH to administer Xacta server for VPN users
Security Tools	VPN	443 / TCP	Web access for VPN users
Security Tools	IronDefense	1514 / UDP	Collect data from various places and log types
Security Tools	n/a	8088 / TCP	VPC Firehouse and Kinesis to collect VPC logs into Splunk from 18.253.138.192/26
Security Tools	Transit gateway	5432 / TCP	Xacta Postgres DB server

FIPS 140-2 Compliance

AWS FIPS-compliant services used in IronNet Collective Defense:

- Cloudwatch
- Cognito
- EKS
- Elasticache
- KDS
- MSK
- RDS
- Route53
- S3
- SNS
- SQS
- VPC

All data is encrypted IAW FIPS 140-2 at rest and in transit

DNSSEC

External DNS services

- IronNet Collective Defense does not provide *external* DNS services
- Customers are responsible for using DNS services that are FedRAMP compliant

Internal DNS services

- Route53 services are configured to provide DNSSEC

Multi-Factor Authentication (MFA)

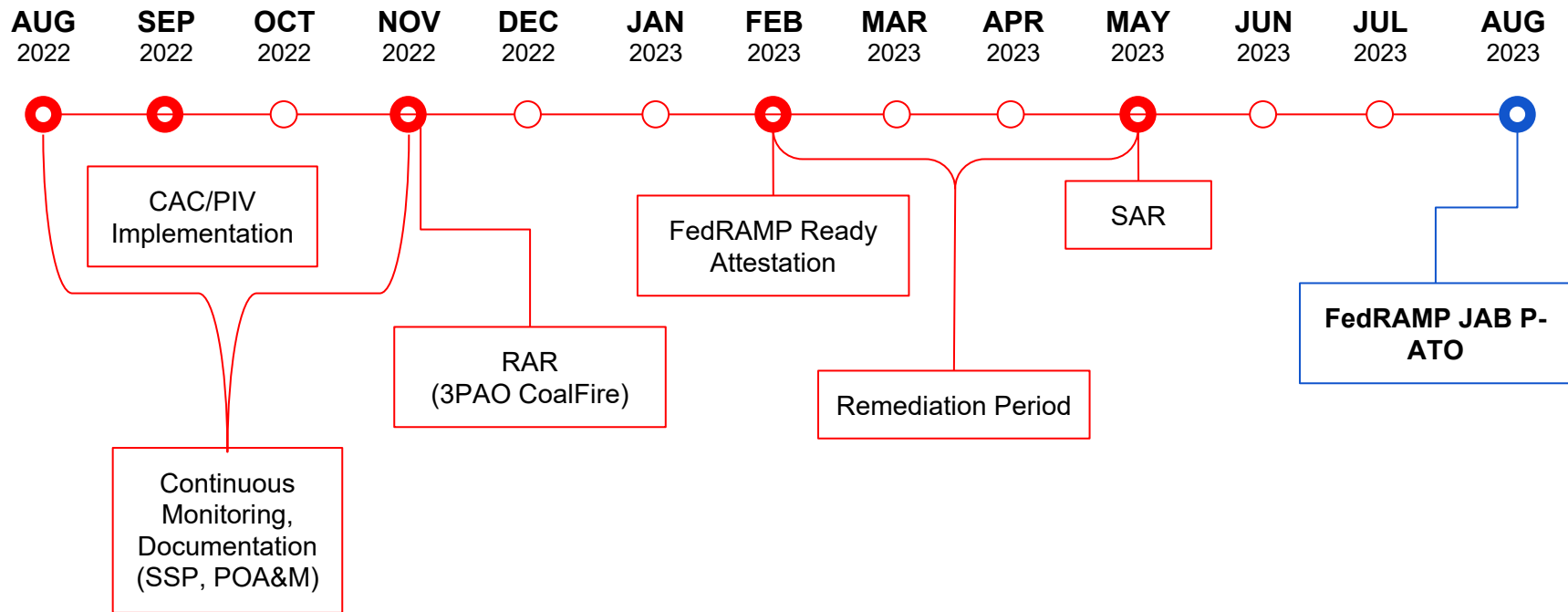
VPC Authentication

- Cognito is configured to require MFA provided by DUO Access Gateway using the Security Assertion Markup Language (SAML)
 - This enables use of DUO hard tokens
- Use of Common Access Card (CAC) planned for a later release

VPN Authentication

- Palo Alto Networks' GlobalProtect is configured to require DUO hard tokens
- Access to the jump host is the same as VPC Authentication above

FedRAMP Readiness Timeline



Thank You!



